AIRNET 300Mb MIMO
Outdoor AP/Bridge

User's Manual

September, 2010

© Copyright 2009 Netkrom Technologies Inc.

Trademark Information

Disclaimer

Netkrom Technologies, Inc. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Netkrom Technologies, Inc. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Netkrom Technologies, Inc will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

FCC NOTICE

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Connect the computer to an outlet on a circuit different from that to which the receiver is connected.
- Increase the separation between the computer and receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC Compliance Statement: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
This device may not cause harmful interference, and
This device must accept any interference received, including interference that may cause undesired operation.

RF Exposure warning

The equipment complies with FCC RF exposure limits set forth for an uncontrolled environment.
The equipment must not be co-located or operating in conjunction with any other antenna or transmitter.

ICES 003 Statement
This Class B digital apparatus complies with Canadian ICES-003.

Declaration of Conformity

Netkrom Technologies, Inc. declares the following:

Product Name: AIRNET 300Mbps a/b/g/n 2.4/5 GHz MIMO Outdoor/AP Bridge

Model No.: AIR-BR600AGN/GNH/ANH conforms to the following Product Standards:

This device complies with the Electromagnetic Compatibility Directive (89/336/EEC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards.)

Electromagnetic Interference (Conduction and Radiation): EN 55022 (CISPR 22)

Electromagnetic Immunity: EN 55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)

Low Voltage Directive: EN 60 950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11: 1997.

Therefore, this product is in conformity with the following regional standards: **FCC Class B:** following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Netkrom Technologies, Inc. also declares that:

The wireless card in this product complies with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following:

EMC Standards: FCC: 47 CFR Part 15, Subpart B, 47 CFR Part 15, Subpart C (Section 15.247); CE: EN 300 328-2, EN 300 826 (EN 301 489-17)

Therefore, this product is in conformity with the following regional standards: **FCC Class B**: following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Manual Version: 2.08c (September 2010)

This manual is written based on Firmware version 2.00

Table of Contents

Overview the Product **7**
Introduction **7**
Features and Benefits 8
Operation Modes and Connection Examples 9
Hardware Installation **14**
Package Contents 14
Setup Requirements 15
AIRNET MIMO Outdoor Bridge Point to Point Installations 16
Mounting AIRNET MIMO Outdoor Bridge in the pole or tower 19
Access the Web Interface **24**
Access with uConfig 24
Access with a Web Browser 27
Navigation **29**
Main Menu Bar 29
How to save changes 29
Basic Network Tab **30**
Network Mode: Bridging and Routing 30
LAN Setup 30
Basic Wireless Tab **33**
Basic Wireless Settings 33
Access Point Parameters Settings 35
Station Parameters Settings 37
Wireless Security 39
Virtual Access Point (VAP) 44
Advance Wireless Tab **45**
Long Range Parameters Setup 45
Advanced Network Tab **47**
Spanning Tree Setup 48
NAT Setup 48
Firewall Setup 50
Multicast Routing Setup 51
Remote Management Setup 51
UPNP: 51
Services Tab **52**
Ping Watchdog 53
Auto-Reboot 53
SNMP Setup 54
NTP Setup 54
Web HTTP Security 54
Telnet Access Setup 55
SSH Access Setup 55
System Log Setup 55

System Tab..56
Firmware Upgrade 56
Host Name 57
Administrative and Read-only Account...57
Configuration Management 58
Device Maintenance...58
Status Page..59
Clients Connection Status in AP Status Info 61
Station Connection Info 62
Status Info 62
More Status 64
VLAN Tab..65
VLAN Switch 65
VLAN Management...66
Appendix I - Network...67
Appendix II – Wireless with Router Mode...70
Appendix III- Advanced Settings 75
Appendix IV- Services 78
Appendix V- VLAN Setup examples 80
A) Tagged Wireless VLAN to Tagged Ethernet VLAN Setup..80
B) Untagged Wireless VLAN to Tagged Ethernet VLAN setup......................................81
C) Tagged VLAN Pass-Through..81

Overview the Product

Introduction

The AIRNET 300Mb MIMO Outdoor AP/Bridge Series is a high-performance Access Point and Bridge designed for enterprises and outdoor users looking for faster throughput and greater coverage. It is backward compatible with IEEE 802.11a/b/g and supports high-speed data transmission up to 300Mbps to accommodate heavy traffic services such as multimedia streaming. Housed in a NEMA6/IP67 waterproof casing, AIRNET 300Mb MIMO Outdoor AP/Bridge Series is designed to withstand any extreme climatic conditions, making it the ideal solution for outdoor applications.

The AIRNET 300Mb MIMO Outdoor AP/Bridge Series has the ability to operate in different operational modes and can be used in a wide variety of wireless applications like Point-to-Point, Point-to-Multipoint, Wireless ISP, and Hot Spot applications. The AIRNET 300Mb MIMO Outdoor AP/Bridge Series meet all these needs with its MIMO technology. The integrated Repeater WDS mode lets you extend the wireless range and coverage of the wireless network feature creates a virtually larger wireless network infrastructure by linking up other access points. Perfect for applications requiring high bandwidth at a fraction of the cost of T1/E1 leased-line, with the additional advantage of zero monthly recurring cost from the service carrier.

Typical usages include bridging satellite offices, corporate LANs, school campus, as well as wireless Internet services, at distances up to 25 miles or 40 Km (without amplifier). The AIRNET 300Mb MIMO Outdoor AP/Bridge also represents the perfect solution for bridging networks that are impossible to connect using wired alternatives, including networks separated by difficult terrains, railroads, or bodies of water.

Depending on the model, some model will have less hardware features. All the software functions are the same.

Features and Benefits

Point-to-Point & Point-to-MultiPoint Support

Point-to-Point communication between different buildings enables you to bridge wireless clients that are kilometers apart while unifying the networks.

Virtual AP (Multiple SSID)

Virtual AP implements mSSID (Multi-SSID) this allows a single wireless card to be set up with multiple virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.

Highly Secured Wireless Network

The AIR-BR600 Series supports the highest available wireless security standard: IEEE802.11i compliant. The AIR-BR600 Series also supports IEEE 802.1x for secure and centralized user-based authentication. Wireless clients are thus required to authenticate through highly secure methods like EAP-TTLS and EAP-PEAP, in order to obtain access to the network.

uConfig Utility

The exclusive uConfig utility allows users to access the user-friendly Web configuration interface of the access point without having to change the TCP/IP setup of the workstation.

HTTPS

The AIR-BR600 Series supports HTTPS (SSL) in addition to the standard HTTP.
HTTPS (SSL) features additional authentication and encryption for secure communication.

Telnet

Telnet allows a computer to remotely connect to the access point CLI (Command Line Interface) for control and monitoring.

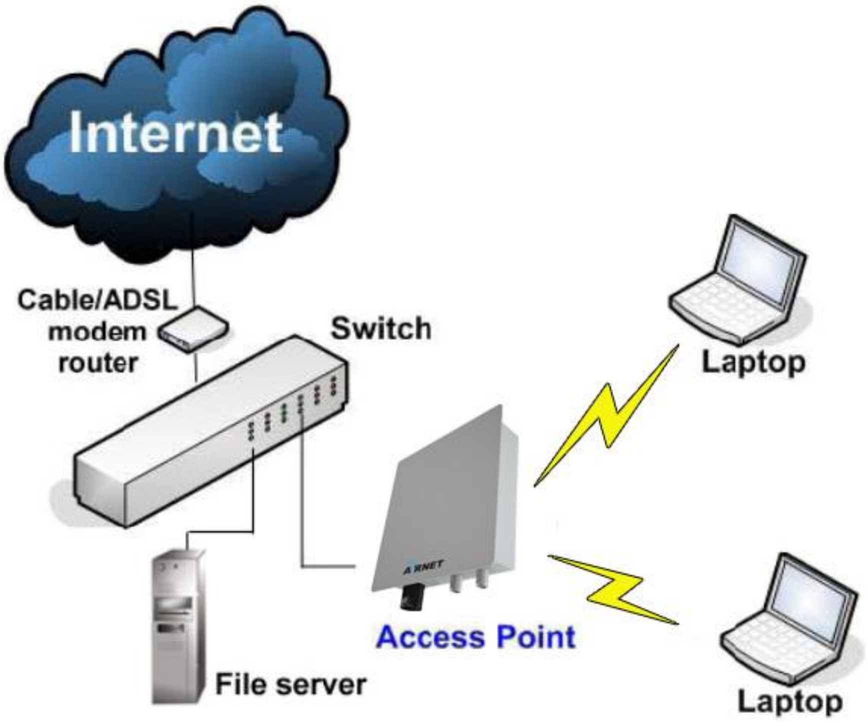
SSH

SSH (Secure Shell Host) establishes a secure host connection to the access point CLI for control and monitoring.

Operation Modes and Connection Examples

Access Point and Access Point WDS Mode

The Access Point Mode is the default mode of the AIR-BR600 Series. It enables the bridging of wireless clients to wired network infrastructure and enables transparent access and communication with each other.
The illustration below shows a typical resources sharing application example using this device. The wireless users are able to access the file server connected to the switch, through the AIR-BR600 Series in Access Point Mode.



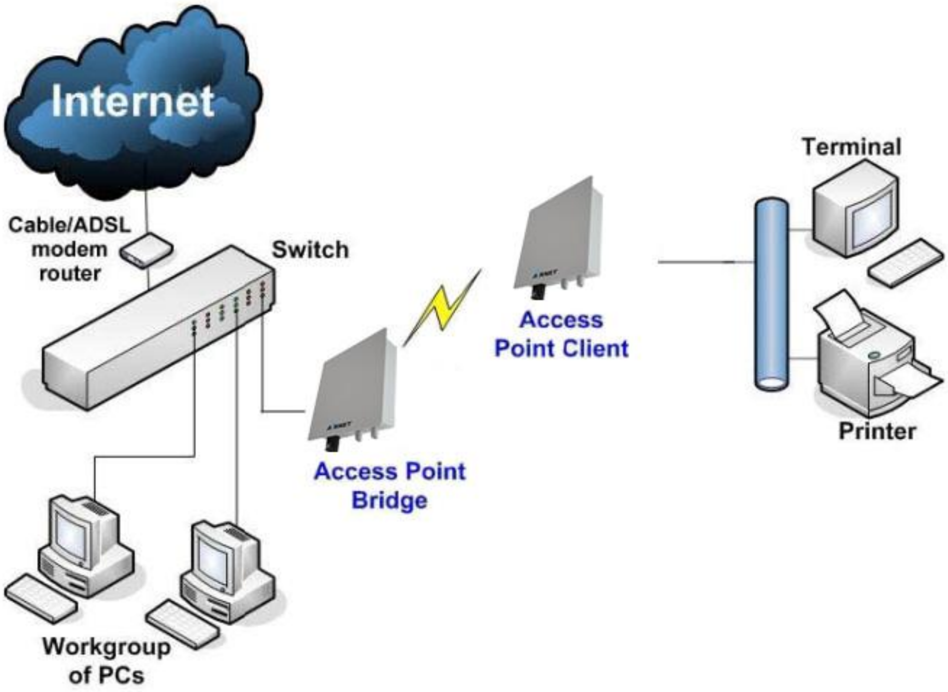
Access Point WDS Mode

This operating mode is generally used for point-to-point or point-to-multi-point connection.
It is mainly used with Station WDS to build the point and multi-point connections.

Station Mode

In **Station** mode the AIR-BR600 Series acts as a wireless client.
When connected to an access point, it creates a network link between the Ethernet network connected at the AIR-BR600 Series, and the wireless Ethernet network connected at the access point.

In this example the workgroup PCs on the Ethernet network connected to the Station device can access the printer across the wireless connection to the access point where the printer is connected.

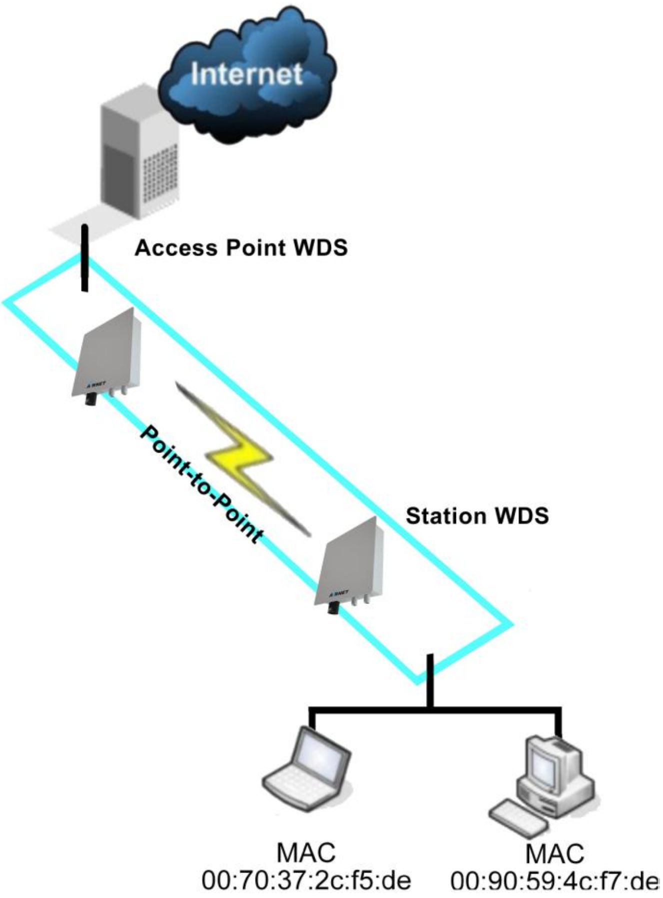


Station WDS Mode

Station WDS mode is similar to Station mode. The difference is that Station WDS must connect to an access point configured as Access Point WDS mode.
Station WDS is mainly used for point-to–point connection between 2 buildings or locations as far as several kilometers away.

Point-to-Point	Point-to-MultiPoint
An access point setup as Access Point WDS and other as Station WDS.	An access point setup as Access Point WDS and several other devices as Station WDS.

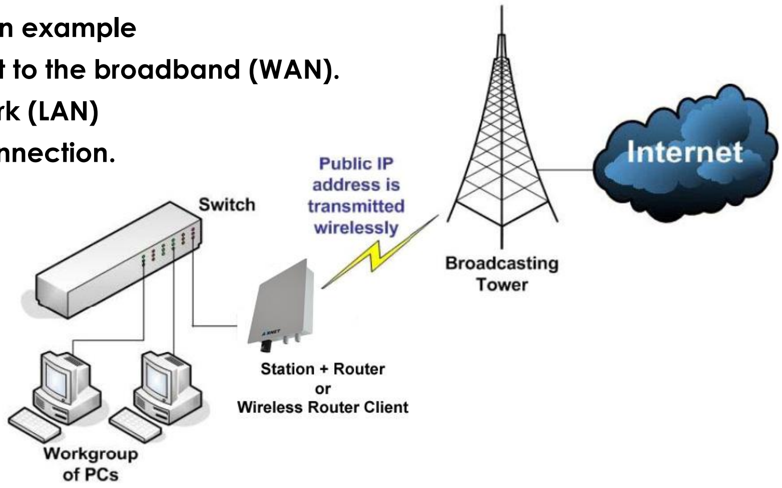
This mode is generally used for outdoor connections over long distances, or for indoor connections between local networks.



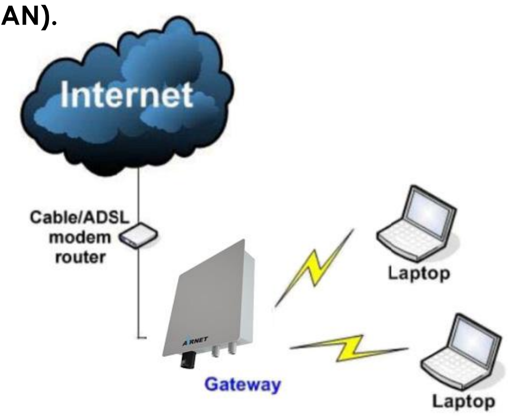
Router Mode

In Router Mode, the AIR-BR600 Series also operates as a router.
Either the wireless or Ethernet can be setup as WAN connection to a broadband modem. Wireless as WAN is known as Station + Router mode and Ethernet as WAN is known as AP + Router mode. The AIR-BR600 Series supports several types of broadband connections Static IP, Dynamic IP and PPPoE. For setup details refer to the respective section.

Station + Router connection example
Wireless is used to connect to the broadband (WAN).
Ethernet is the local network (LAN)
sharing the Broadband connection.


Internet
Public IP address is transmitted wirelessly
Switch
Broadcasting Tower
Station + Router or Wireless Router Client
Workgroup of PCs

AP + Router connection example
Ethernet is use to connect to the broadband (WAN).
Wireless is the local network (LAN)
sharing the broadband connection.



Broadband Internet Access Type:

Static IP Address

Use Static IP Address you have subscribed a fixed IP or range IP addresses from your ISP.

Dynamic IP Address

With Dynamic IP Address the device automatically request IP address from modem or ISP.

PPP over Ethernet (PPPoE)

When using ADSL services provided by your ISP support PPPoE connection.

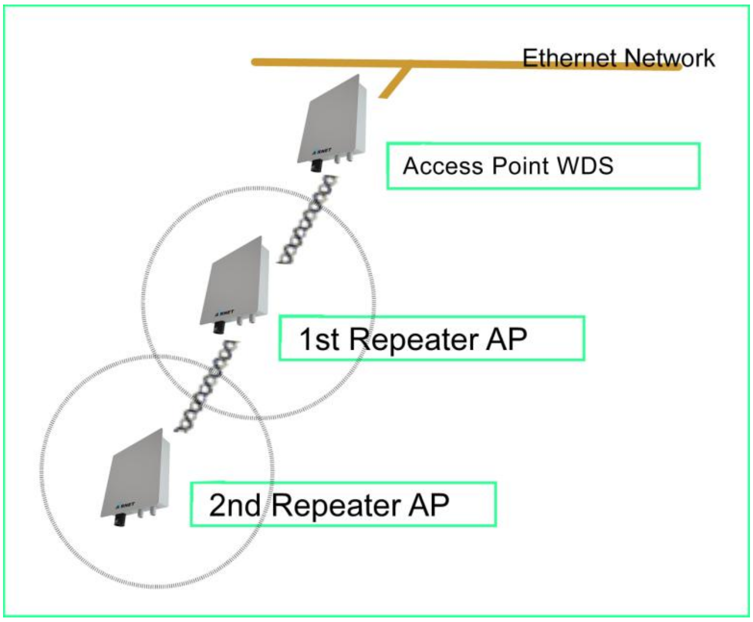
Repeater WDS Mode

Repeater WDS Mode is mainly used to extend the wireless range and coverage of the wireless network allowing access and communications over places generally difficult for wireless clients to connect to the network.

In Repeater mode, the AIR-BR600 Series acts as a relay for network signals on the network by regenerating the signals it receives, and retransmitting them to main network infrastructure.

Detailed information on the Repeater mode is available in the Repeater Setup section.

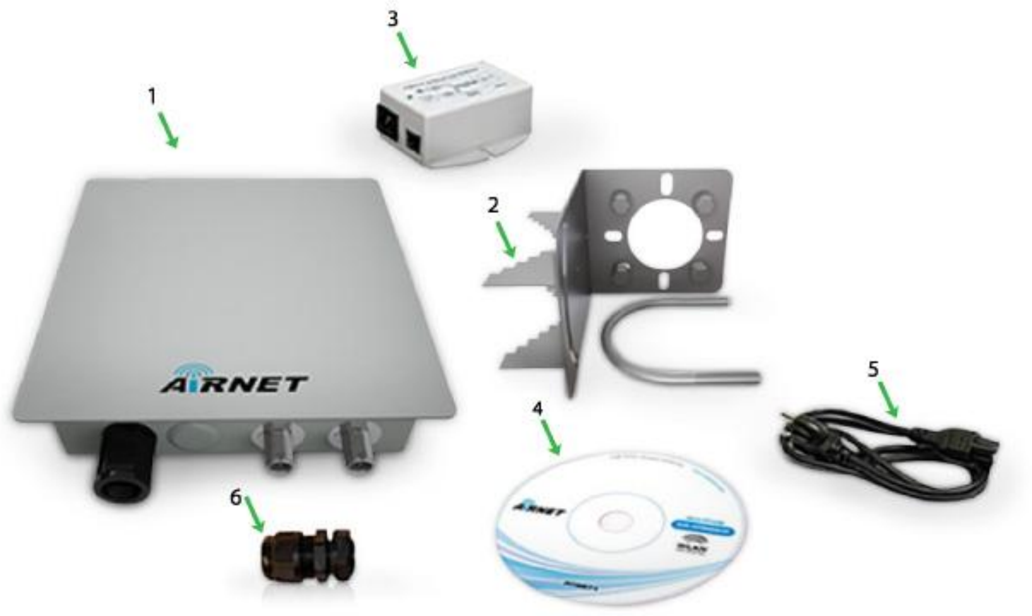
**** Note: Repeater WDS requires the access point to be setup in Access Point WDS mode to work.**



Hardware Installation

Package Contents

Take a moment to ensure you have all of the following parts in your AIRNET 300Mb MIMO Outdoor AP/Bridge installation kit before you begin installing the product. If any parts are missing, please contact your local vendor or contact us at 305-4182232.



KIT CONTAINS

1. AIRNET 300Mbps MIMO Outdoor AP/Bridge Bridge
2. Mounting brackets (include: 1 Wall/ Pole mounting system and 4 screw nuts)
3. PoE Injector
4. Power Cable
5. RJ45 Waterproof Connector System
6. CD ROM

Setup Requirements

- CAT5/5e Networking Cable.
- At least 1 computer installed with a web browser and a wired or wireless network interface adapter.
- All network nodes installed with TCP/IP and properly configured IP address parameters.

Important!

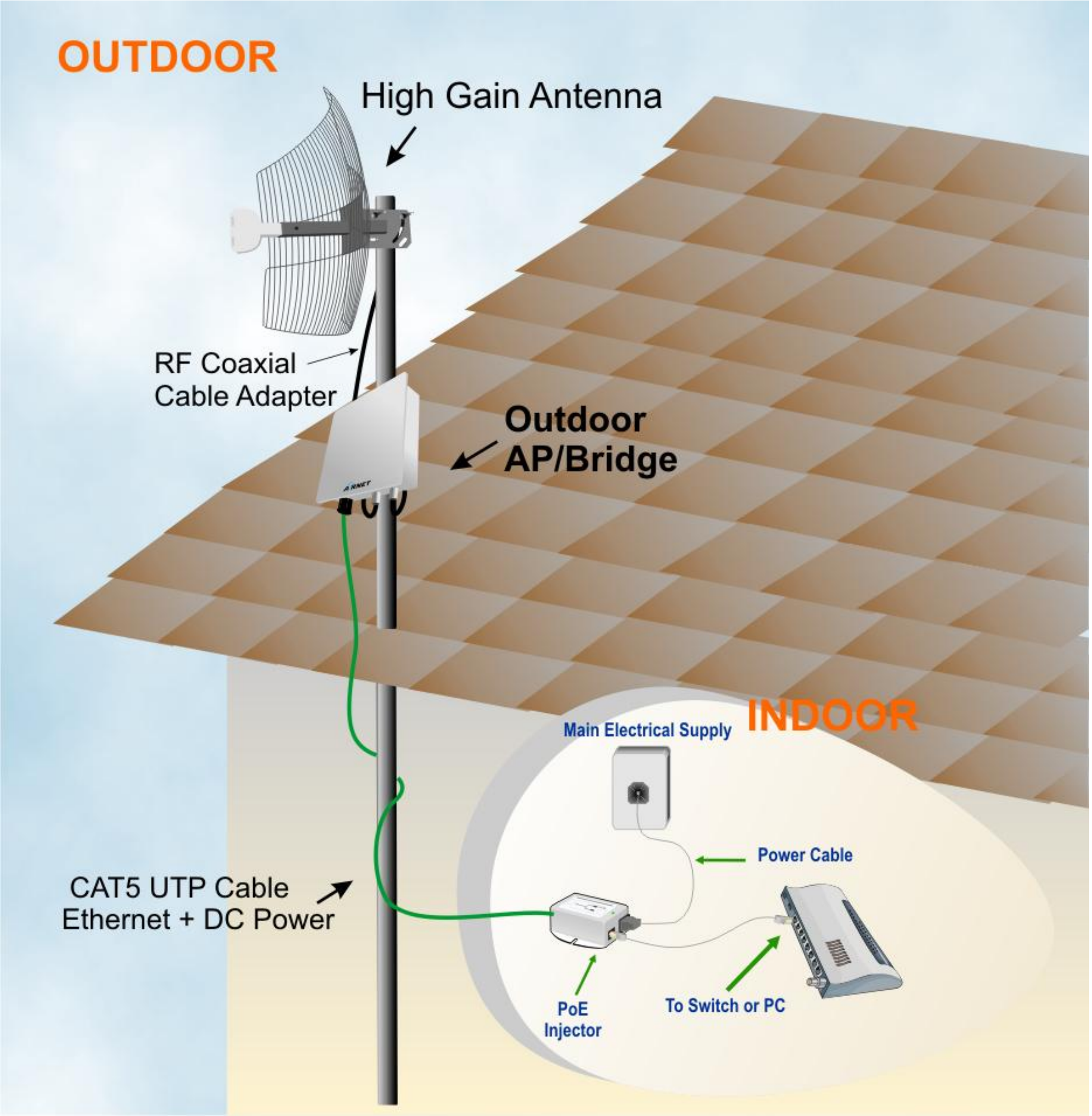
- Configure and verify the AIRNET MIMO Outdoor Bridge operations first before you mount the unit in a remote location.

- You may need to install a lightning arrestor to protect your AIRNET MIMO Outdoor Bridge from the lightning.

- For choosing the best location for your AIRNET MIMO Outdoor Bridge choose an elevated location where trees, buildings and large steel structures will not obstruct the antenna signals and which offers maximum line-of-sight propagation with the users.

AIRNET MIMO Outdoor Bridge Installations

The diagram below shows the overall setup of AIRNET MIMO Outdoor Bridge unit.

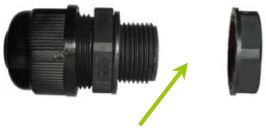


Step 1:

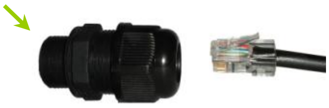
Connect your UTP or FTP Outdoor cat.5 Ethernet cable with waterproof connector to the RJ-45 connector on the AIRNET MIMO Outdoor Bridge unit. Then connect the other end of the cable to the PoE injector.

For the Netkrom PoE, the recommended length of the RJ45 Category 5 cable is up to 150 feet or 50 meters.

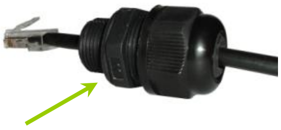
1.- Remove the thin enclosure nut from the feedthru assembly. This can be discarded. Loosen the compression nut completely



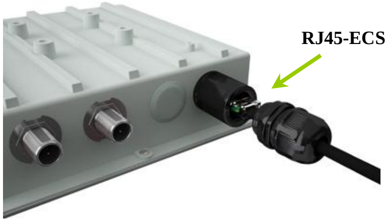
2.- Insert the RJ45 connector thru the feedthru assembly



3.- Tighten the compression nut loosely to the feedthru assembly



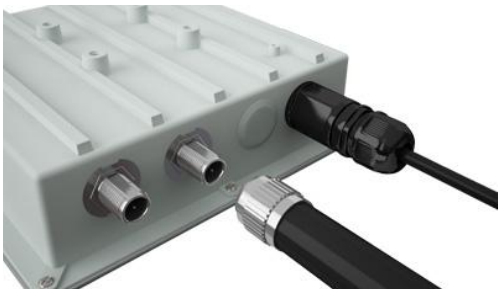
4.- Screw the entire feedthru assembly into the RJ45-ECS housing which is already mounted in the AIRNET MIMO Outdoor Bridge unit. There should be a rubber gasket between the two assemblies. Tighten the feedthru assembly to create a seal.

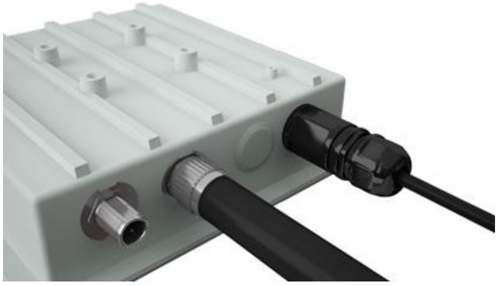


5.- The final step is to tighten the compression nut until the gaskets are tight around the Cat5 cable. Always push the cable toward the connector while tightening to ensure good strain relief of cable to connector.

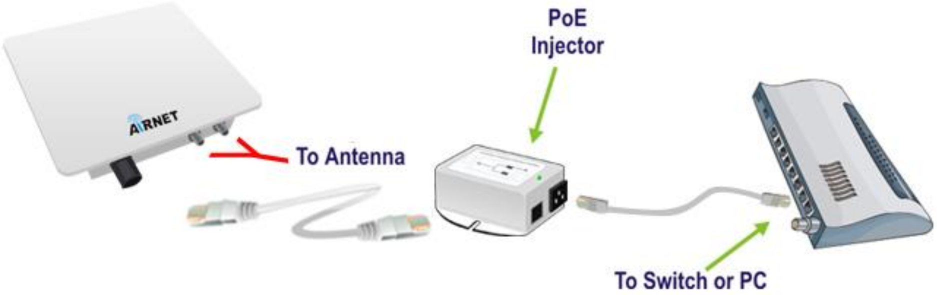
Step 2:

Connect the external antenna to the N Female connector of the access point.



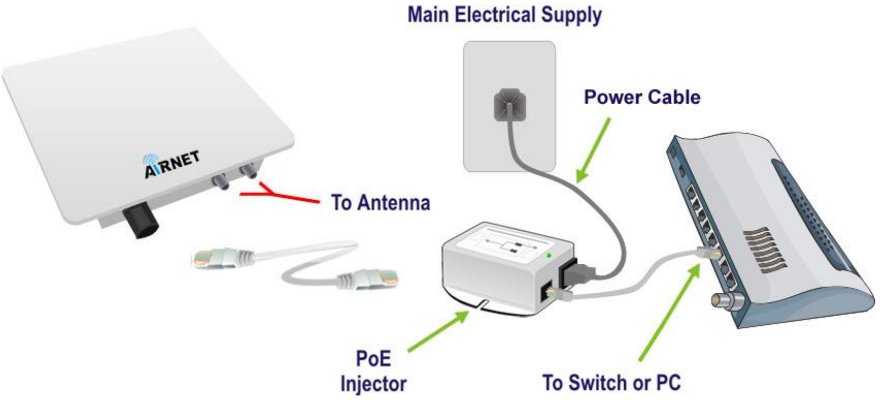


From the PoE injector connect one cat.5 Ethernet cable to the radio and another cat.5 cable to a switch or PC.



Connect the power cable supplied in the Netkrom PoE kit to the main electrical supply and the power plug into the socket of the injector.
Now, turn on your power supply. Notice that the POWER LED has lighted up. This indicates that the access point is receiving power through the Netkrom PoE Injector and that connection between your access point and your network has been established.

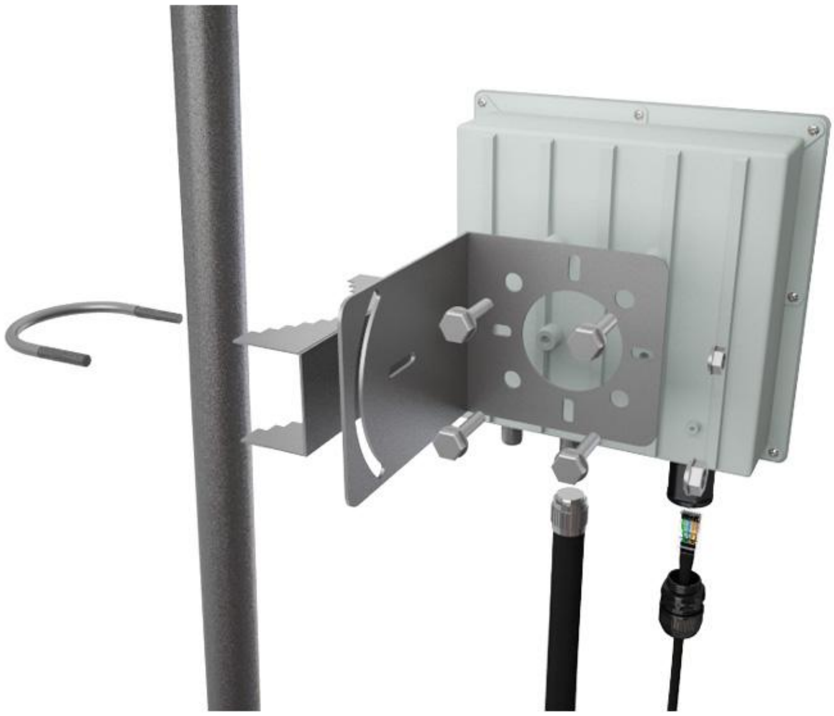
Note:
Please use the PoE injector provided in the package. Using a PoE with a different voltage rating will damage this product.



Mounting AIRNET MIMO Outdoor Bridge in the pole or tower

Netkrom AIRNET MIMO Outdoor Bridge device can be mounted on the pole or tower as shown in following:

1.- Mount the bracket to the pole.
2.- Attach the radio to the bracket which was mounted on the pole with the supplied nuts and 4 screws.



Configure the IP Address

After setting up the hardware you need to assign an IP address to your PC so that it is in the same subnet as the access point.

For Windows 95/98/98SE/ME/NT

Step 1:

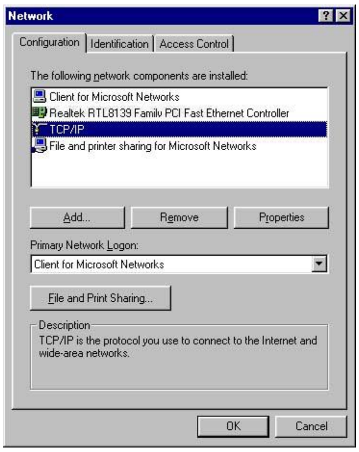
From your desktop, right-click the **Network Neighborhood** icon and select **Properties**.

Step 2:

Select the network adapter that you are using, then right-click and select **Properties**.

Step 3:

Highlight **TCP/IP** and click on the **Properties** button.



The following network components are installed:

- Client for Microsoft Networks
- Realtek RTL8139 Familv PCI Fast Ethernet Controller
- TCP/IP
- File and printer sharing for Microsoft Networks

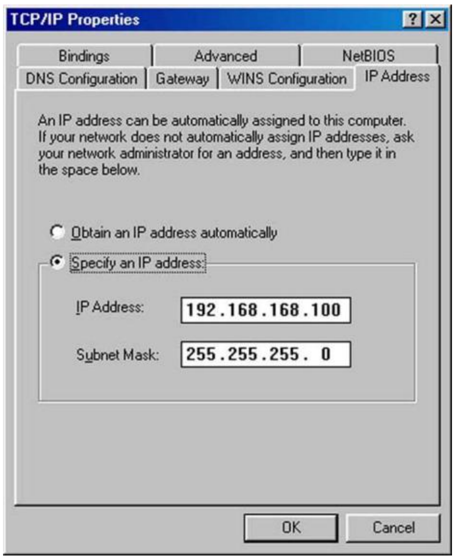
Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Step 4:

Select the **Specify an IP address** radio button.

Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically
● Specify an IP address:

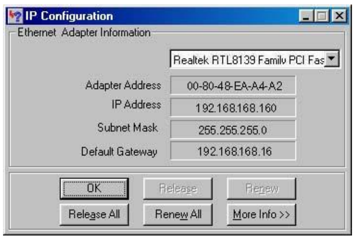
IP Address: 192.168.168.100

Subnet Mask: 255.255.255. 0

Step 5:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, select **Run**, and enter the command: *winipcfg*.

Select the Ethernet adapter from the drop-down list and click **OK**.



IP Configuration

Ethernet Adapter Information

Realtek RTL8139 Familv PCI Fas

Adapter Address 00-80-48-EA-A4-A2
IP Address 192.168.168.160
Subnet Mask 255.255.255.0
Default Gateway 192.168.168.16

PC is now setup with proper IP address to communicate with the access point.

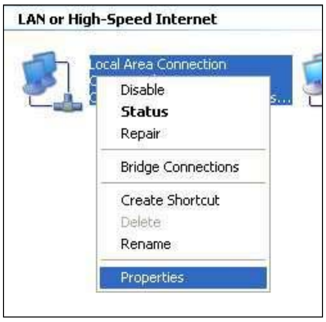
For Windows XP/2000

Step 1:

Go to your desktop, right-click on the **My Network Places** icon and select **Properties**.

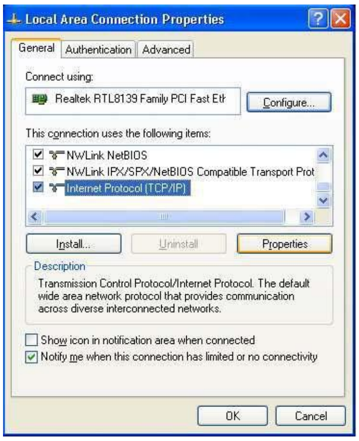
Step 2:

Right-click the network adapter icon and select **Properties.**



Step 3:

Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.


Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

- ☑ NWLink NetBIOS
- ☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

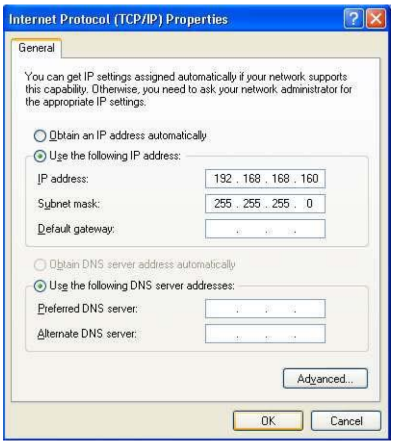
☐ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

Step 4:

Select the **Use the following IP address** radio button.

Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.


Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 168 . 160

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

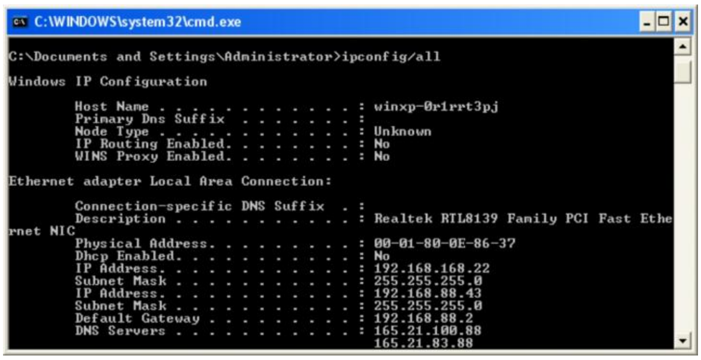
Alternate DNS server: . . .

Step 5:

Click on the **OK** button to close all windows.

Step 6:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, **Accessories**, select **Command Prompt**, and type the command: *ipconfig/all*



```
C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : winxp-0r1rrt3pj
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
        Physical Address. . . . . . . . . : 00-01-80-0E-86-37
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.168.22
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 192.168.88.43
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.88.2
        DNS Servers . . . . . . . . . . . : 165.21.100.88
                                            165.21.83.88
```

PC is now setup with a proper IP address to communicate with the access point.

Access the Web Interface

Access with uConfig

The UConfig utility provides direct access to the web interface.

Step 1:

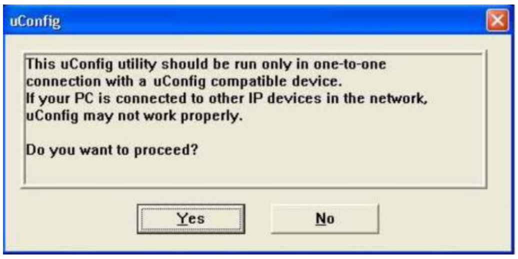
Insert the Product CD into your CD-ROM drive, the CD will autorun.

Step 2:

From the **Utilities** section, select to install the **uConfig** utility to your hard disk.

Step 3:

After installation double-click on the **uConfig** icon and click on the **Yes** button.

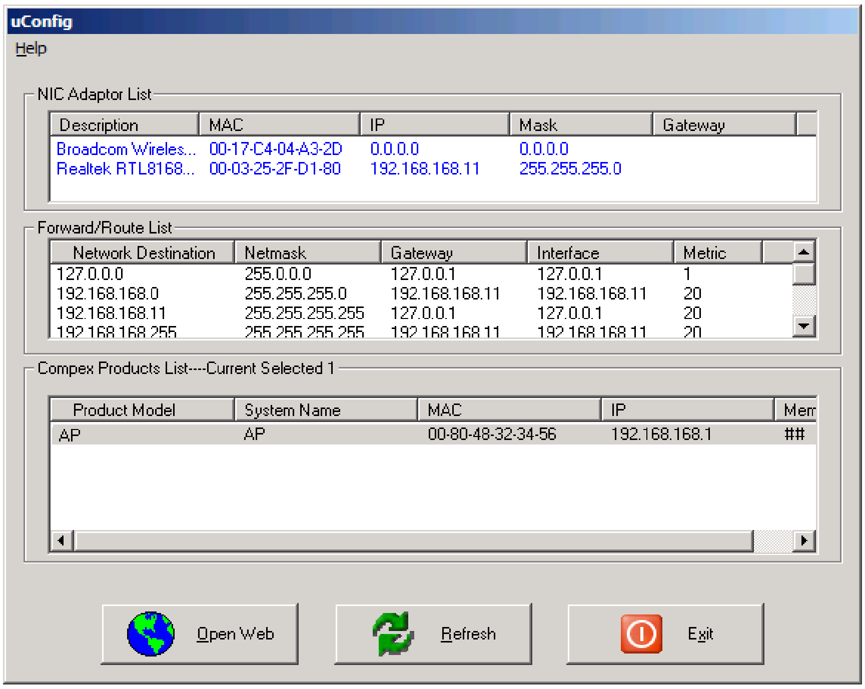


This uConfig utility should be run only in one-to-one connection with a uConfig compatible device.
If your PC is connected to other IP devices in the network, uConfig may not work properly.

Do you want to proceed?

Step 4:

Select the access point from the products list and click on the **Open Web** button. To retrieve and display the latest device(s) in the list, click on the **Refresh** button.



NIC Adaptor List

Description	MAC	IP	Mask	Gateway
Broadcom Wireles...	00-17-C4-04-A3-2D	0.0.0.0	0.0.0.0	
Realtek RTL8168...	00-03-25-2F-D1-80	192.168.168.11	255.255.255.0	

Forward/Route List

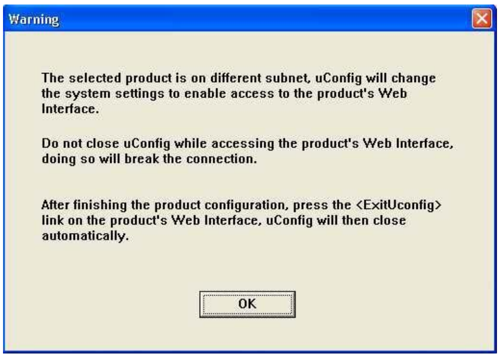
Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.168.0	255.255.255.0	192.168.168.11	192.168.168.11	20
192.168.168.11	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.168.255	255.255.255.255	192.168.168.11	192.168.168.11	20

Compex Products List----Current Selected 1

Product Model	System Name	MAC	IP	Mem
AP	AP	00-80-48-32-34-56	192.168.168.1	##

Step 5:

Do not exit the uConfig program while accessing the web-based interface as this will disconnect you from the device. Click on the **OK** button.



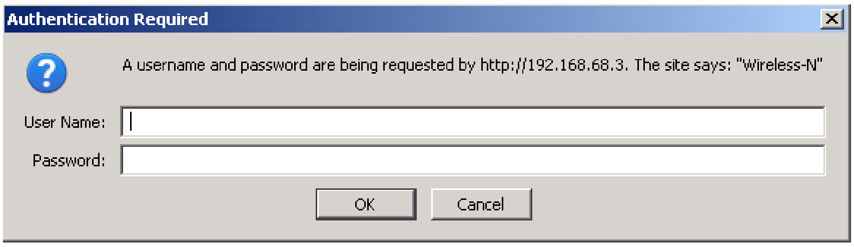
The selected product is on different subnet, uConfig will change the system settings to enable access to the product's Web Interface.

Do not close uConfig while accessing the product's Web Interface, doing so will break the connection.

After finishing the product configuration, press the <ExitUconfig> link on the product's Web Interface, uConfig will then close automatically.

Step 6:

At the login prompt, enter the User Name and Password.
The default are :
User Name : **admin**
Password : **password**



Authentication Required

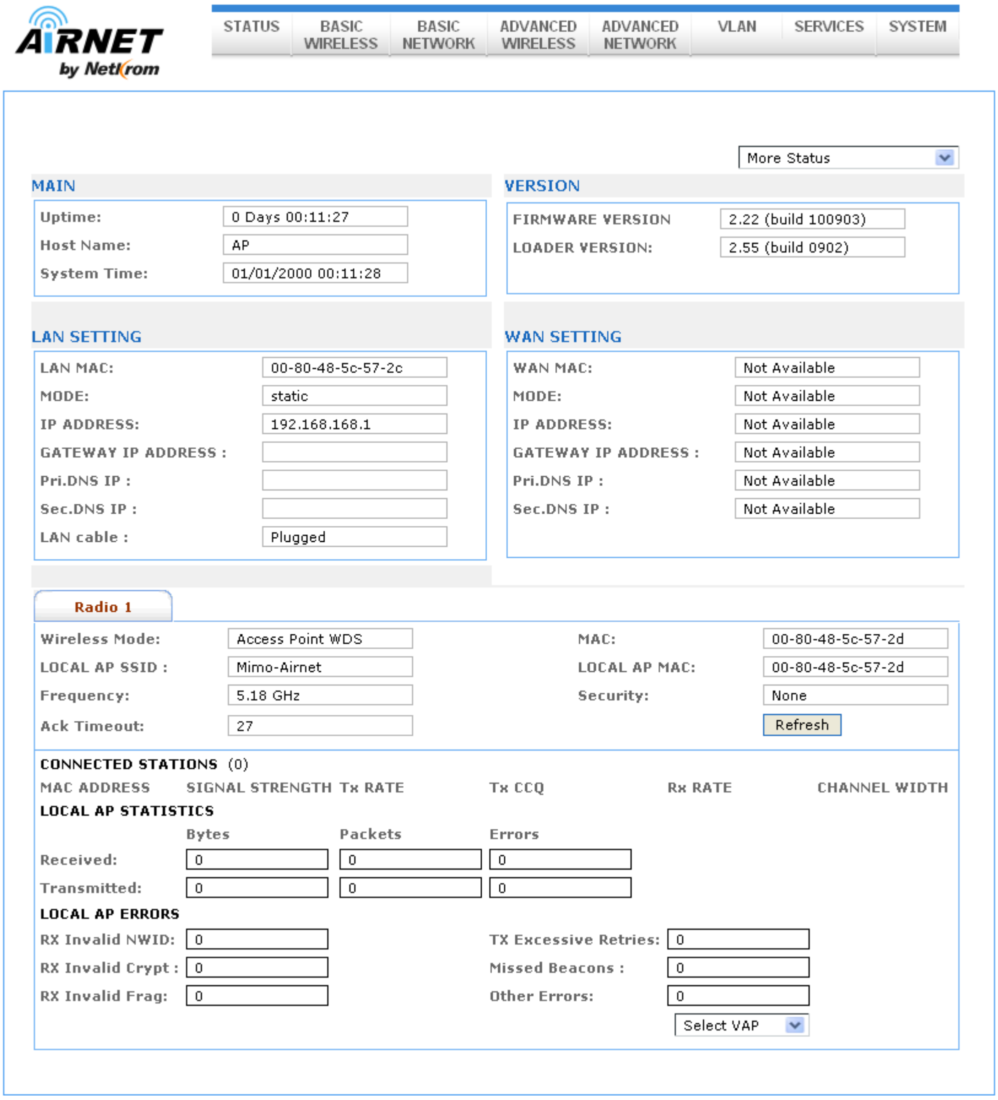
A username and password are being requested by http://192.168.68.3. The site says: "Wireless-N"

User Name:

Password:

Step 7:

It then opens the device home page. The Status page.



MAIN

Uptime:	0 Days 00:11:27
Host Name:	AP
System Time:	01/01/2000 00:11:28

VERSION

FIRMWARE VERSION	2.22 (build 100903)
LOADER VERSION:	2.55 (build 0902)

LAN SETTING

LAN MAC:	00-80-48-5c-57-2c
MODE:	static
IP ADDRESS:	192.168.168.1
GATEWAY IP ADDRESS :	
Pri.DNS IP :	
Sec.DNS IP :	
LAN cable :	Plugged

WAN SETTING

WAN MAC:	Not Available
MODE:	Not Available
IP ADDRESS:	Not Available
GATEWAY IP ADDRESS :	Not Available
Pri.DNS IP :	Not Available
Sec.DNS IP :	Not Available

Radio 1

Wireless Mode:	Access Point WDS	MAC:	00-80-48-5c-57-2d
LOCAL AP SSID :	Mimo-Airnet	LOCAL AP MAC:	00-80-48-5c-57-2d
Frequency:	5.18 GHz	Security:	None
Ack Timeout:	27		Refresh

CONNECTED STATIONS (0)

MAC ADDRESS SIGNAL STRENGTH Tx RATE Tx CCQ Rx RATE CHANNEL WIDTH

LOCAL AP STATISTICS

	Bytes	Packets	Errors
Received:	0	0	0
Transmitted:	0	0	0

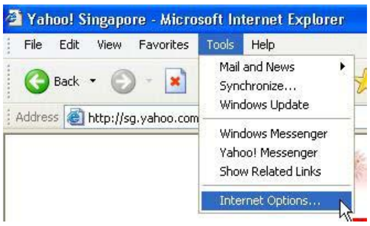
LOCAL AP ERRORS

RX Invalid NWID:	0	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

Access with a Web Browser

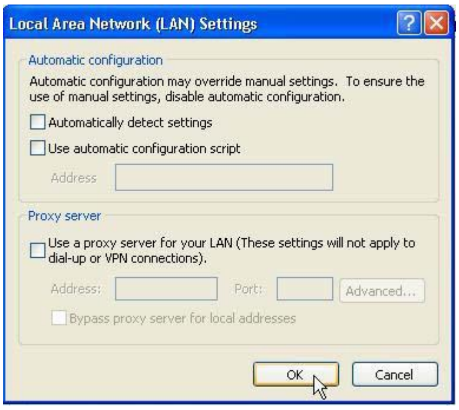
Step 1:

Launch your Web browser. e.g. MS Internet Explorer, FireFox, Netscape, etc..
For MS IE, under the **Tools** tab, select **Internet Options.**



Step 2:

Open the **Connections** tab and in the **LAN Settings** section disable all the option boxes. Click on the **OK** button to update the changes.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: Advanced...

☐ Bypass proxy server for local addresses

OK Cancel

Step 3:

At the **Address** bar type in http://192.168.168.1 and press **Enter** on your keyboard.

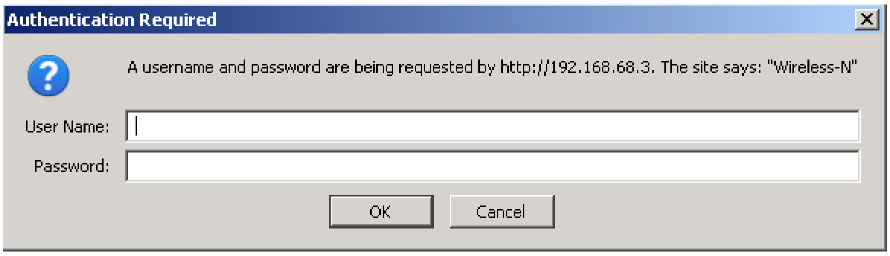
Step 4:

At the login prompt, enter the User Name and Password.

The default are :

User Name : **admin**

Password : **password**



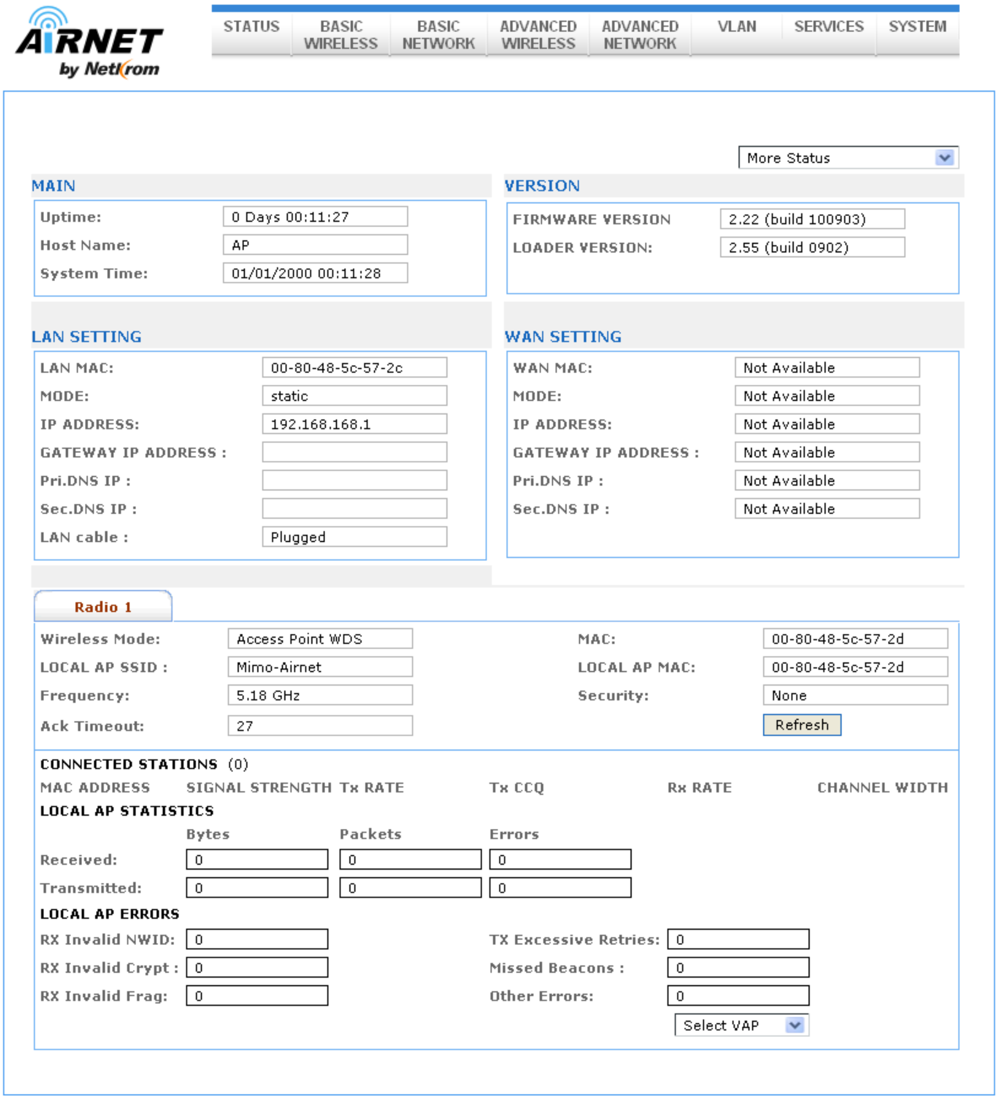
Authentication Required

A username and password are being requested by http://192.168.68.3. The site says: "Wireless-N"

User Name: |

Password:

It then opens the device home page. The Status page.



MAIN

Uptime:	0 Days 00:11:27
Host Name:	AP
System Time:	01/01/2000 00:11:28

VERSION

FIRMWARE VERSION	2.22 (build 100903)
LOADER VERSION:	2.55 (build 0902)

LAN SETTING

LAN MAC:	00-80-48-5c-57-2c
MODE:	static
IP ADDRESS:	192.168.168.1
GATEWAY IP ADDRESS :	
Pri.DNS IP :	
Sec.DNS IP :	
LAN cable :	Plugged

WAN SETTING

WAN MAC:	Not Available
MODE:	Not Available
IP ADDRESS:	Not Available
GATEWAY IP ADDRESS :	Not Available
Pri.DNS IP :	Not Available
Sec.DNS IP :	Not Available

Radio 1

Wireless Mode:	Access Point WDS	MAC:	00-80-48-5c-57-2d
LOCAL AP SSID :	Mimo-Airnet	LOCAL AP MAC:	00-80-48-5c-57-2d
Frequency:	5.18 GHz	Security:	None
Ack Timeout:	27		

CONNECTED STATIONS (0)

MAC ADDRESS	SIGNAL STRENGTH	Tx RATE	Tx CCQ	Rx RATE	CHANNEL WIDTH

LOCAL AP STATISTICS

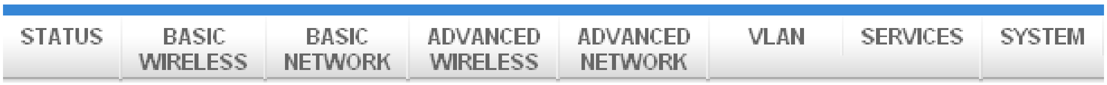
	Bytes	Packets	Errors
Received:	0	0	0
Transmitted:	0	0	0

LOCAL AP ERRORS

RX Invalid NWID:	0	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

Navigation

Main Menu Bar



Status: Page displays current status of the device and the statistical information.

Basic Wireless: Page contains the controls for a wireless network configuration, while covering basic wireless settings which define operating mode, associating details and data security options.

Basic Network: Page covers the configuration of network operating mode, IP settings and network services (i.e. DHCP Server).

Advanced Wireless: Page settings for more advanced wireless features.
Advanced Network page settings for more advanced network features.

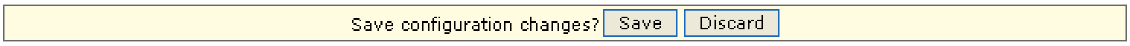
Services: Page covers the configuration of system management services (i.e. Ping Watchdog, Auto-Reboot, SNMP, NTP, Telnet, SSH, System Log).

System: Page contains controls for system maintenance routines, administrator account management, device customization and configuration backup.

How to save changes

After made changes from each respective setup page, click this button,

After that, the prompt below appears. You are asked to confirm if you want to save the change permanently into the device flash.

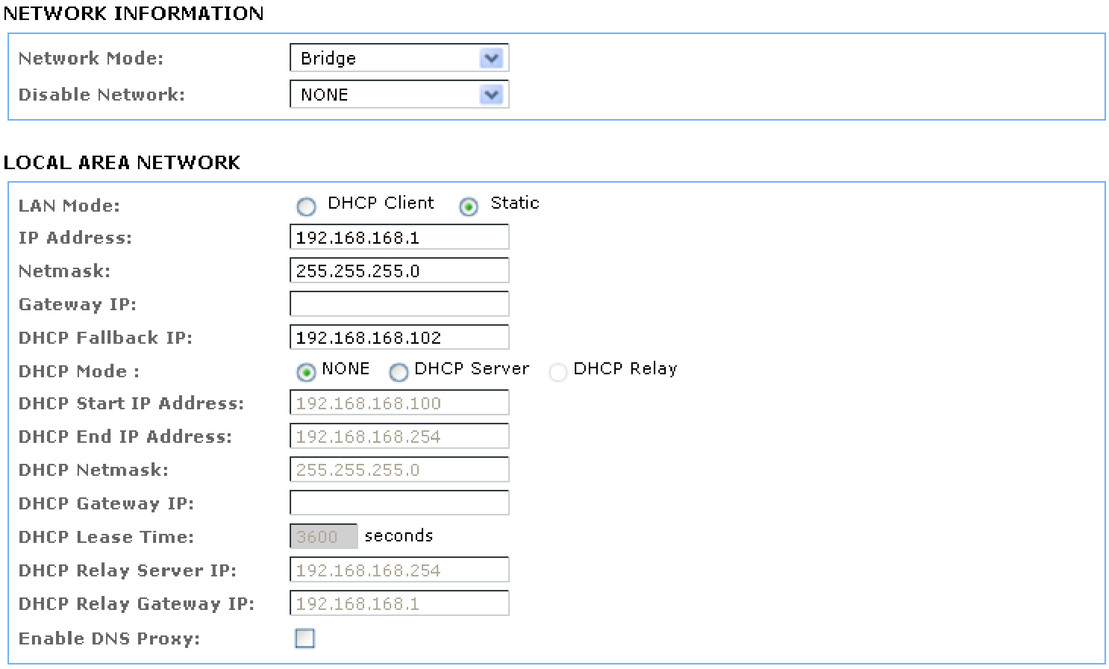


Save configuration changes?

Click **Save** will write all configuration changes to flash.
Click **Discard** will discard all changes made.
If you are not sure what changes were made earlier, it’s recommend to discard and reconfigure again.

Basic Network Tab

Click **BASIC NETWORK** from the menu bar to open the page as show below.



NETWORK INFORMATION

Network Mode:	Bridge
Disable Network:	NONE

LOCAL AREA NETWORK

LAN Mode:	○ DHCP Client ● Static
IP Address:	192.168.168.1
Netmask:	255.255.255.0
Gateway IP:	
DHCP Fallback IP:	192.168.168.102
DHCP Mode :	● NONE ○ DHCP Server ○ DHCP Relay
DHCP Start IP Address:	192.168.168.100
DHCP End IP Address:	192.168.168.254
DHCP Netmask:	255.255.255.0
DHCP Gateway IP:	
DHCP Lease Time:	3600 seconds
DHCP Relay Server IP:	192.168.168.254
DHCP Relay Gateway IP:	192.168.168.1
Enable DNS Proxy:	□

Network Mode: Bridging and Routing

Network Mode:

Select between Bridge (default) and Router mode.

LAN Setup

LAN Mode:

Static: (default) lets you enter a specific IP address for the device.

Default IP address is 192.168.168.1

DHCP Client: when set let device learn the IP address automatically from the network.

Netmask:

Let you set the class for the IP address set.

Default class C and value is 255.255.255.0

Gateway: (optional)

Enter the gateway IP address of the network the device is connected.

DHCP Fallback IP:

Should device in **DHCP Client** mode failed to obtain an IP address from the DHCP server, user can access device using this temporary fallback IP address.

DHCP Mode:

None: function disabled

DHCP Server: Check to enable. Device act IP address distribution server automatically issue IP address and other network information to the DHCP Client request them.

DHCP Relay: check to enable. Enter the IP address of the remote DHCP server where the DHCP Client request will be relayed to.

DHCP Start IP Address:

Enter the starting IP address to be issue.

DHCP End IP Address:

Enter the last IP address the server will issue.

DHCP Netmask:

Let you set the IP class for the IP address range set for the start and end address.

*** Note:-** if device is also the router then IP class must be same as device IP class.

DHCP Lease Time: (default is **3600** seconds or 1hour)

Enter the new lease time in seconds.

DHCP Relay Server IP:

Enter the IP address of the remote DHCP server where the DHCP Client request will be relay to get the IP address.

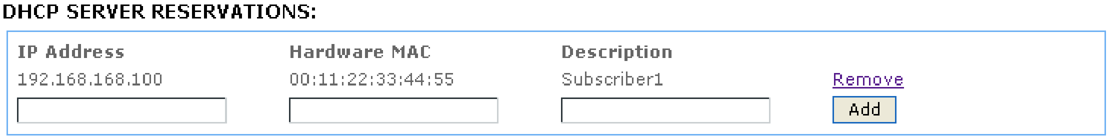
DHCP Relay Gateway IP:

Enter the IP address of the remote gateway where the DHCP Client request will be relay to get the gateway IP address.

Enable DNS Proxy:

Check to enable function. Device router operation will act as proxy to resolve all DNS requests.

DHCP Reservations



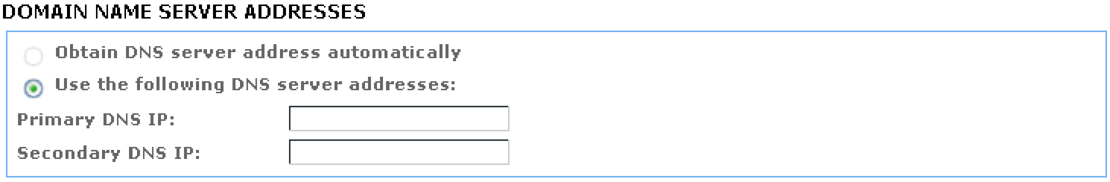
DHCP SERVER RESERVATIONS:

IP Address	Hardware MAC	Description	
192.168.168.100	00:11:22:33:44:55	Subscriber1	Remove
			Add

Click **Add** to enter for each device the IP address and MAC address.

All DHCP active lease devices are displayed in the **Status** tab page from the **More Status** selection.

Domain Name Server Entry



DOMAIN NAME SERVER ADDRESSES

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Primary DNS IP:

Secondary DNS IP:

The Primary and Secondary DNS IP addresses entry is for device operation to resolve domain name to reach certain servers like internet time server and other services that use domain name.

* Note: Ensure device gateway IP is also set that to allow device to access to internet.

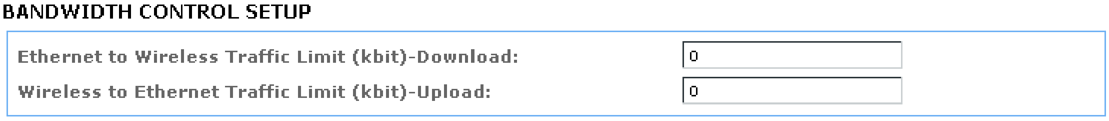
Primary DNS IP: (optional)

Enter the primary DNS IP address nearest to the gateway router.

Secondary DNS IP: (optional)

Enter the secondary DNS IP address nearest to the gateway router.

Bandwidth Control between Ethernet and Wireless



BANDWIDTH CONTROL SETUP

Ethernet to Wireless Traffic Limit (kbit)-Download:	0
Wireless to Ethernet Traffic Limit (kbit)-Upload:	0

An entry of value “0” means no bandwidth flow limit between the 2 interfaces.

An entry of “2048” means 2048Kbit or 2Mbit limit traffic flow between the 2 interfaces.

Default is “0”

Basic Wireless Tab

Under the tab, there is the selection of 4 radios.

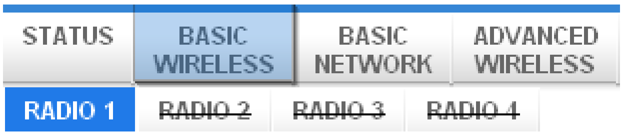


Fig 2.1 Basic Wireless Tab

Currently device supports only one 802.11n radio card. Select **RADIO 1** to configure.
Basic Wireless Tab contains all the wireless setup, which is necessary for the operator to setup the wireless part of the link.

Enable the radio

☑ Enable Radio 1

Fig 2.2 Enable Radio Checkbox

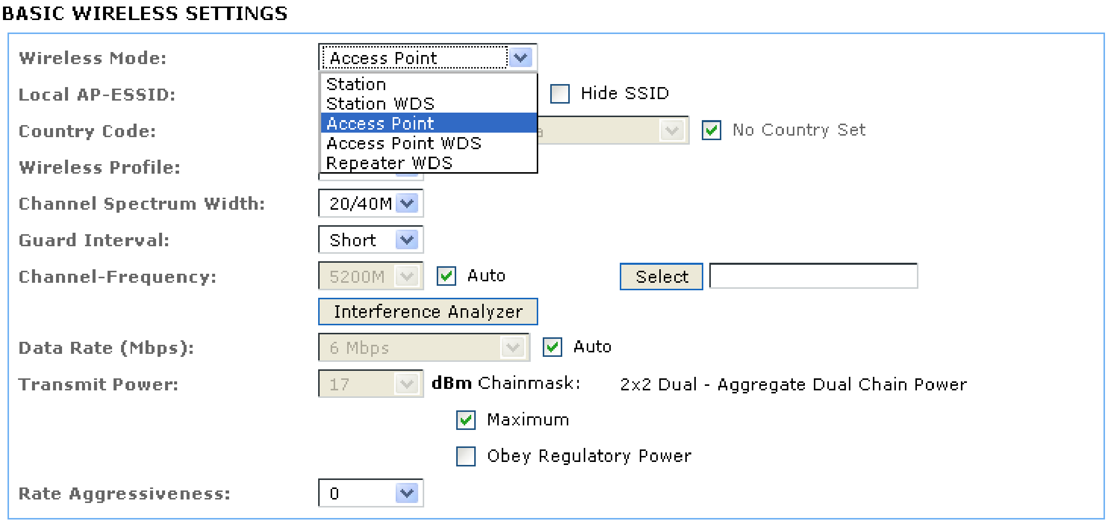
Tick/Untick the checkbox to enable/disable the radio.

Basic Wireless Settings

All the basic wireless settings can be configured in this page. Operators can change the ESSID, regulatory country code, wireless profile, channel spectrum width, frequency of interest, data rates, transmit power and rate aggressiveness.

Wireless Mode

There are **5 modes** available.



BASIC WIRELESS SETTINGS

Wireless Mode: Access Point

Station
Station WDS
Access Point
Access Point WDS
Repeater WDS

Local AP-ESSID: □ Hide SSID

Country Code: ☑ No Country Set

Wireless Profile:

Channel Spectrum Width: 20/40M

Guard Interval: Short

Channel-Frequency: 5200M ☑ Auto Select

Interference Analyzer

Data Rate (Mbps): 6 Mbps ☑ Auto

Transmit Power: 17 dBm Chainmask: 2x2 Dual - Aggregate Dual Chain Power

☑ Maximum

□ Obey Regulatory Power

Rate Aggressiveness: 0

Access Point

This mode can be connected to **Station** mode, and then forwards all the traffic to the network devices connected to the Ethernet devices of the Station.

Access Point WDS

This mode can be connected to Station WDS mode. Using WDS protocol, it allows a client or station device to bridge wireless traffic transparently.

Station:

This is a client mode that can be connected to the Access Point mode. It is used to bridge the wireless connection to an Access Point. It forwards all the traffic to/from the network devices to the Ethernet interface. This mode translates all the packets that pass through device to its own MAC address, thus resulting in a lack of transparency.

Station WDS:

WDS is the acronym of Wireless Distribution System. It can be connected to the **Access Point WDS** mode. It enables packet forwarding at layer 2 level. Unlike Station mode, it is fully transparent at layer 2 level.

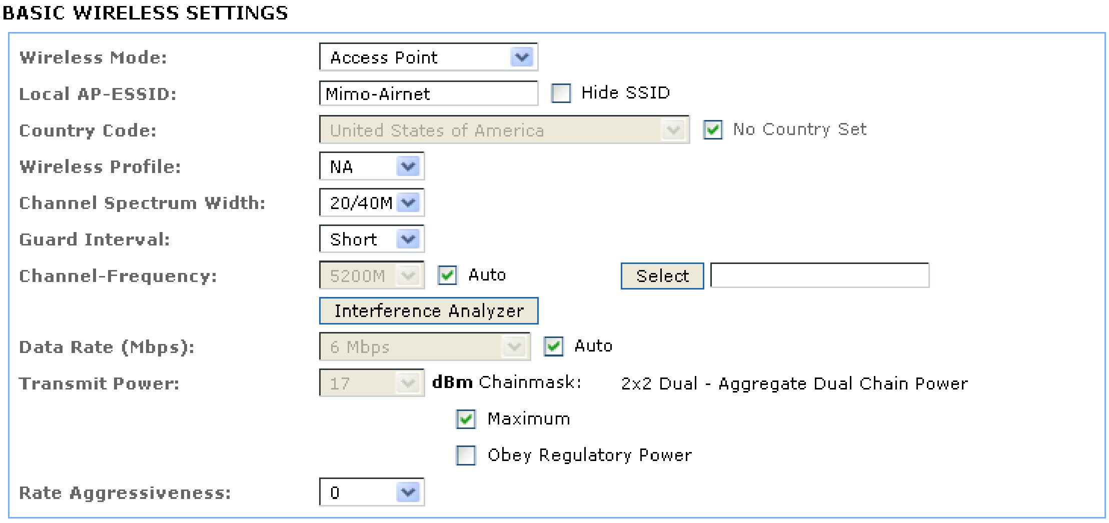
****Note:- for Station WDS, Access Point WDS, Repeater WDS:**
WDS protocol used is not defined as the standard, thus compatibility issues between equipment from different vendors might arise.

Repeater WDS

This mode consists of a Station WDS and an Access Point WDS mode. The Repeater WDS must first link up with an Access Point WDS, and then it can link up with a Station WDS. It acts as an extension to the link and can add more Repeater WDS as necessary.

***Note:- for Repeater WDS: ESSID must be the same for the Remote AP and the Local AP. The channels used in the Repeater to link to another Repeater will follow the Access Point WDS connection selected channel.**

Access Point Parameters Settings



BASIC WIRELESS SETTINGS

Wireless Mode: Access Point

Local AP-ESSID: Mimo-Airnet □ Hide SSID

Country Code: United States of America ☑ No Country Set

Wireless Profile: NA

Channel Spectrum Width: 20/40M

Guard Interval: Short

Channel-Frequency: 5200M ☑ Auto Select

Interference Analyzer

Data Rate (Mbps): 6 Mbps ☑ Auto

Transmit Power: 17 dBm Chainmask: 2x2 Dual - Aggregate Dual Chain Power

☑ Maximum

□ Obey Regulatory Power

Rate Aggressiveness: 0

Fig 2.3 Basic Wireless Settings (Access Point/ Access Point WDS)

Local AP-ESSID

This is the Service Set Identifier used to identify the operator's wireless LAN. It should be specified while operating in Access Point or Access Point WDS mode.

All the client devices within its range will receive broadcast messages from the access point advertising this SSID.

Hide SSID:

Once checked, this will disable advertising the SSID of the access point in broadcast messages to wireless stations. This option is only available in Access Point, Access Point WDS and Repeater WDS mode only.

Country Code

Different countries have different power levels and frequency selections. To ensure device operation follows regulatory compliance rules, operator to select correct country code where device will be used. The channel list, output power limits, IEEE 802.11 and Channel-Spectrum Width modes will be tuned according to regulations of the selected country.

No Country Set:

Option when checked; only the frequency range is available.

11n 2.4GHz is 2412-2462MHz, 11n 5GHz is 5180-5320MHz and 5745-5825MHz.

Wireless Profile:

NA is 11n 5GHz band and represents a mixed of 802.11n and 802.11a mode.

NG is 11n 2.4GHz band and represents a mixed of 802.11n, 802.11g and 802.11b mode.

Channel Spectrum Width

20M represents the data transmitted at a bandwidth of 20MHz. 20/40MHz represents the data transmitted at either 20MHz or 40MHz. In very noisy environment it automatically falls back to 20MHz from 40MHz to be more resilient to the interference.

In situation when auto fallback did not happen, manually changing channel spectrum width to 20MHz will help reducing interference on the link and improve performance.

*** Note: 40MHz bandwidth is non-standard for 802.11n/g mode operation. If you experience unstable performance change Channel Spectrum Width to 20M.**

Guard Interval: Guard band between packets. For long distant connection, select Long for better performance.

Channel – Frequency

This is frequency selection you can set for device to operate on. The frequency range available depends on the country domain you select in Country Code. For 5GHz frequency range some have DFS characteristics earmarked by regulations. Selecting one of these frequencies for operation may affect and delay of 2 minutes or more (possibly up to 10 minutes in some situations) for device to attempt to establish a connection.

Auto*:* When checked, during startup, device automatically selects the least interfering channels (or frequency) for the operation.

Data Rate

Data Rates consist of both the legacy rates and the MCS (Modulation Coding Scheme – Only for 802.11n) rates.

6 – 54Mbps are Legacy Rates
MCS0 to MCS7 are 802.11n rates, which uses only 1 stream.
MCS8 to MCS15 are 802.11n rates, which uses 2 streams.

Auto*:* The data rate selected will follow an advanced rate algorithm that takes into condition the amount of errors at the data rate and fine tune to the best data rate it can use.

Transmit Power

The maximum transmit power displayed is determined by the country code and the maximum transmit power of the device that is being used.

Note on changing channels:

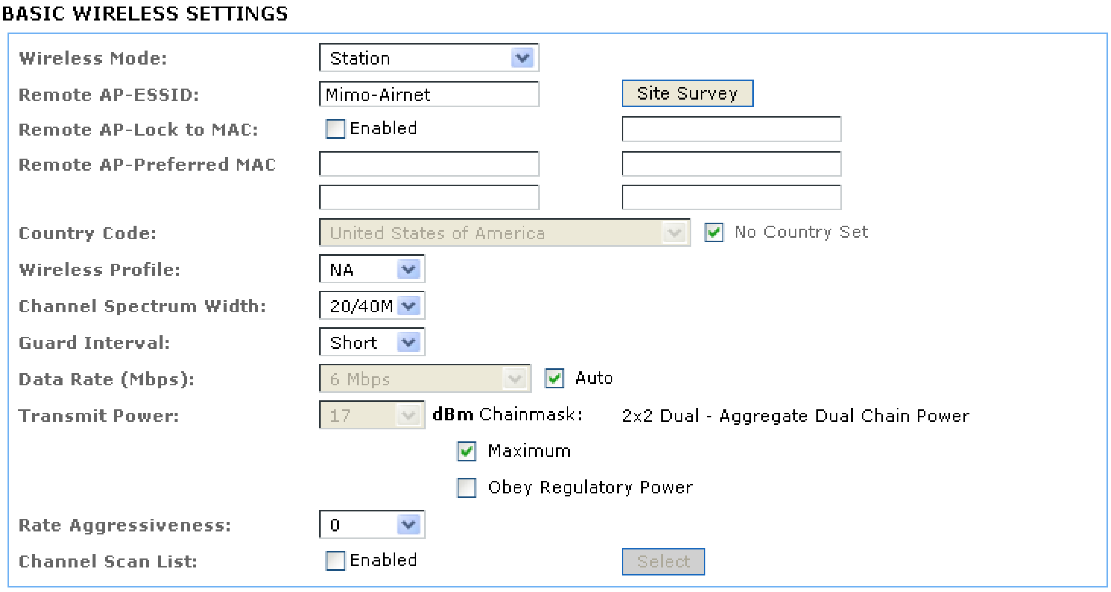
When the operator changes the channels and if this new frequency have higher output power permitted by regulation, the power previously selected low power level will remain unchanged.
You need to readjust the power level in order to take advantage of higher output power available for the channel.

Maximum: checking this box will result in maximum Tx output power overriding regulation.
Obey Regulatory Power: checking this box will obey Tx output regulatory power by country.

Rate Aggressiveness

Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm.
There are 2 scenarios Rate Aggressiveness is useful. Environment might be noisy at times.
Lower the throughput will ensure better stability. Rate Aggressiveness allows device to reduce the transmit rate, so range or power can be higher. Choose a range of value from -3,-2,-1.
Environment might be free of interference. But fully auto algorithm might give lower throughput.
Increase aggressiveness will increase transmit rate in this case to get higher throughput.
Choose a range of value from +3, +2, +1.

Station Parameters Settings



BASIC WIRELESS SETTINGS

Wireless Mode:	Station	
Remote AP-ESSID:	Mimo-Airnet	Site Survey
Remote AP-Lock to MAC:	□ Enabled	
Remote AP-Preferred MAC		
Country Code:	United States of America	☑ No Country Set
Wireless Profile:	NA	
Channel Spectrum Width:	20/40M	
Guard Interval:	Short	
Data Rate (Mbps):	6 Mbps	☑ Auto
Transmit Power:	17 dBm Chainmask:	2x2 Dual - Aggregate Dual Chain Power
	☑ Maximum	
	□ Obey Regulatory Power	
Rate Aggressiveness:	0	
Channel Scan List:	□ Enabled	Select

Fig 2.4 Basic Wireless Settings (Station/Station WDS)

This options below are only available in **Station, Station WDS** and **Repeater WDS** modes unless otherwise stated.

Wireless Mode: Station

Remote AP-ESSID

This is the Service Set Identifier used by station to seek and connect to the access point of same the SSID identifier.

Site Survey

Site Survey will search for the available wireless networks in range on all the supported channels and will allow you to select one for association. In case the selected network uses encryption, you’ll need to set security parameters in wireless security section. Click Scan to re-scan the Access Points in range. Select the Access Point from the list and click Close this window. Site Survey channel scan list can be modified using the Channel Scan List control.

Remote AP – Lock to MAC

Enter the MAC address of the remote access point the device is connected to. This option will make device only connect to this access point. This is important when connection is Point-to-Point operation.

Remote AP - Preferred MAC

Enter the preferred MAC address of the access point you want device to connect when it first startup. Up to max of 4 MAC addresses can be entered. Priority is from top to bottom. In the event all preferred MAC addresses are not available, device will then pick the matching SSID access point with the strongest signal.

Country Code

Different countries have different power levels and also frequency selections. To ensure device operation follows regulatory compliance rules, the operator should make sure that correct country code where device will be used, is selected. The channel list, output power limits, IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country. **Station setting must match AP country code setting.**

No Country Set:

Option when checked, only the frequency range are available.

11n 2.4GHz is 2412-2462MHz, 11n 5GHz is 5180-5320MHz and 5745-5825MHz.

Wireless Profile:

NA is 11n 5GHz band and represents a mixed of 802.11n and 802.11a mode.

NG is 11n 2.4GHz band and represents a mixed of 802.11n, 802.11g and 802.11b mode.

** **Station setting must match AP Wireless Profile setting.**

Channel Spectrum Width

20M represents the data transmitted at a bandwidth of 20MHz. 20/40MHz represents the data transmitted at either 20MHz or 40MHz. In very noisy environment it automatically falls back to 20MHz to be more resilient to the interference. In situation when auto fall back did not happened, manually changing channel spectrum width to 20MHz will to help reduce interference on the link and improve performance.

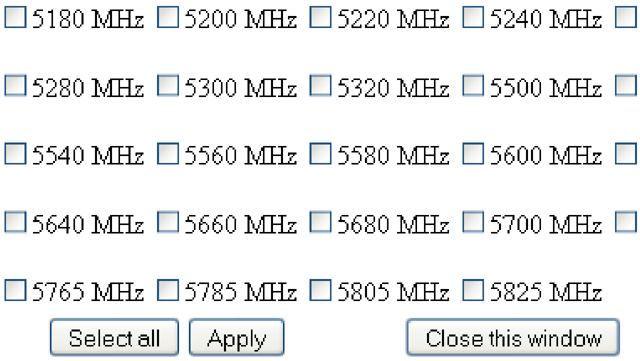
*** Note: 40MHz bandwidth is non-standard for 802.11n/g mode operation. If you experience unstable performance change Channel Spectrum Width to 20M.**

** **Station setting must match AP Channel Spectrum Width setting.**

Maximum: checking this box will result in maximum Tx output power overriding regulation.

Obey Regulatory Power: checking this box will obey Tx output regulatory power by country.

Channel Scan List



□ 5180 MHz □ 5200 MHz □ 5220 MHz □ 5240 MHz □ 5260 MHz

□ 5280 MHz □ 5300 MHz □ 5320 MHz □ 5500 MHz □ 5520 MHz

□ 5540 MHz □ 5560 MHz □ 5580 MHz □ 5600 MHz □ 5620 MHz

□ 5640 MHz □ 5660 MHz □ 5680 MHz □ 5700 MHz □ 5745 MHz

□ 5765 MHz □ 5785 MHz □ 5805 MHz □ 5825 MHz

Fig 2.5 Channel Scan List (In US Country Code)

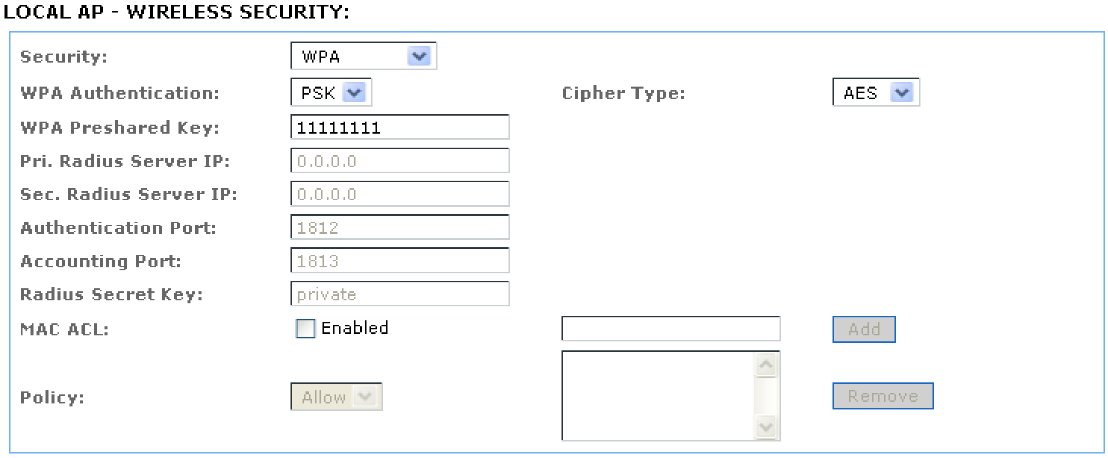
Mark on box to enable **Channel Scan List**

User can then mark and selective only those frequencies station will scan the AP to increase scan speed. However, ensure the frequencies selected are available at the AP setup.

Wireless Security

All the wireless security settings are set under this section.
The operation of the Keys is the same for ALL the Wireless modes.

WPA or WPA2 Authentication



LOCAL AP - WIRELESS SECURITY:

Security: WPA
WPA Authentication: PSK
Cipher Type: AES
WPA Preshared Key: 11111111
Pri. Radius Server IP: 0.0.0.0
Sec. Radius Server IP: 0.0.0.0
Authentication Port: 1812
Accounting Port: 1813
Radius Secret Key: private
MAC ACL: □ Enabled
Policy: Allow

Fig 2.7 WPA (Access Point/Access Point WDS/Repeater WDS)

WPA PSK

PSK (Default) – WPA or WPA2 with Pre-shared Key method.

Cipher Type

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

AES - Advanced Encryption Standard (AES) algorithm.

AUTO (Default) – Automatically select between both algorithms.

Preshared Key

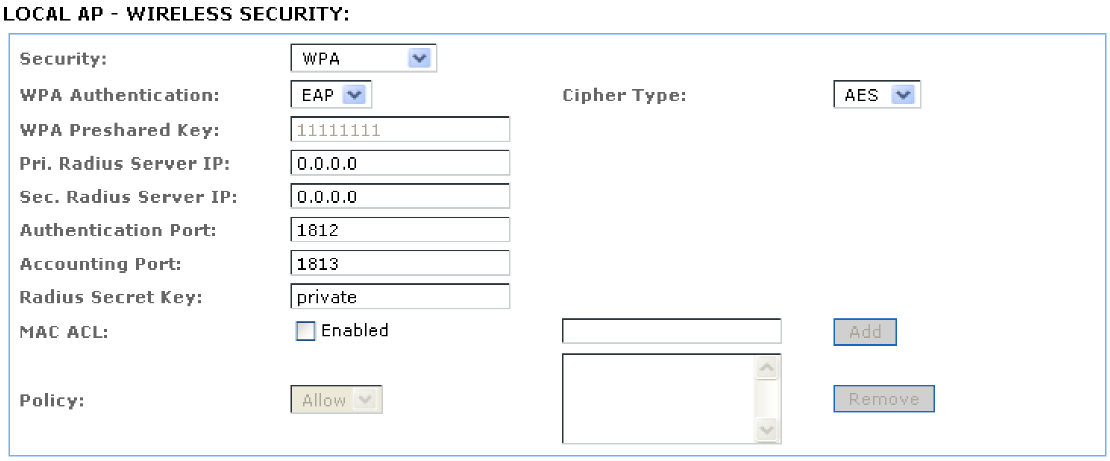
This option is available when **WPA** or **WPA2**, with **PSK** selected.

The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

*** Important:

802.11n network using WPA authentication should use AES cipher type for connection. Only AES allows highest transmission speed and throughput operation.
Using TKIP cipher type device will limit maximum transmission speed of up to 54Mbps only.

WPA + EAP



LOCAL AP - WIRELESS SECURITY:

Security:	WPA		
WPA Authentication:	EAP	Cipher Type:	AES
WPA Preshared Key:	11111111		
Pri. Radius Server IP:	0.0.0.0		
Sec. Radius Server IP:	0.0.0.0		
Authentication Port:	1812		
Accounting Port:	1813		
Radius Secret Key:	private		
MAC ACL:	□ Enabled		Add
Policy:	Allow		Remove

Fig 2.8 WPA + EAP

EAP – WPA or WPA2 with EAP (Extensible Authentication Protocol)

Firmware supported options for clients are: EAP-TTLS and EAP-PEAP

Cipher Type

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

AES - Advanced Encryption Standard (AES) algorithm.

AUTO (Default) – Automatically select between both algorithms.

Primary Radius Server IP

Enter the Primary Radius Server IP address.

Secondary Radius Server IP

Enter the Secondary Radius Server IP address.

Authentication Port

Enter the Authentication Port number of the Radius Server. Default is 1812.

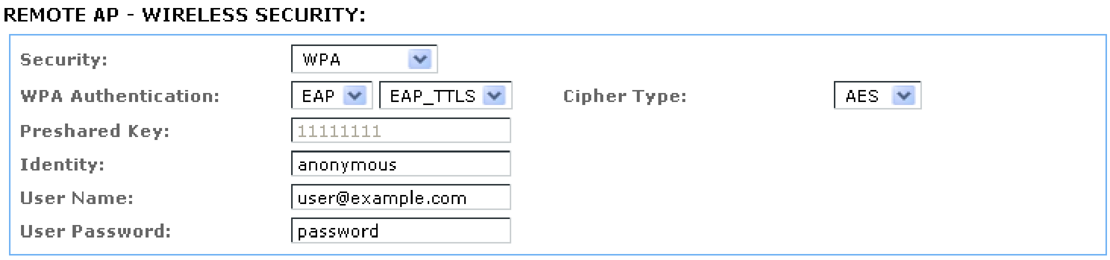
Accounting Port

Enter the Accounting Port number of the Radius Server. Default is 1813.

Radius Secret Key

Enter the Secret Key to match with Radius Server key. Device use this to authenticate itself to the Radius Server.

WPA EAP-TTLS and WPA EAP-PEAP



REMOTE AP - WIRELESS SECURITY:

Security:	WPA		
WPA Authentication:	EAP EAP_TTLS	Cipher Type:	AES
Preshared Key:	11111111		
Identity:	anonymous		
User Name:	user@example.com		
User Password:	password		

Fig 2.8 WPA (Station /Station WDS/Repeater WDS)

This applies to the following modes only, when **WPA** or **WPA2**, with **EAP** is selected.

Station, Station WDS, Repeater WDS mode.

Identity

Identification credential used by the wpa-supplicant for EAP authentication.

User Name:

Identification credential used by the wpa-supplicant for EAP tunneled authentication in unencrypted form.

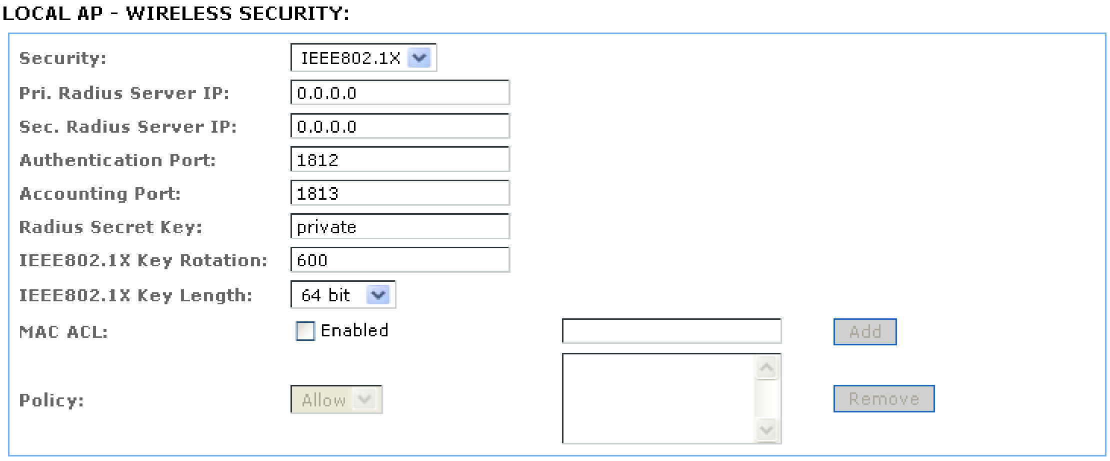
User Password:

Password credential used by the wpa-supplicant for EAP authentication

IEEE802.1x Settings

The operation of the Keys is the same for ALL the modes.

**** Note: Operating with IEEE802.1x security will limit AP to maximum wireless link speed of 54Mbps only.**



LOCAL AP - WIRELESS SECURITY:

Security:	IEEE802.1X
Pri. Radius Server IP:	0.0.0.0
Sec. Radius Server IP:	0.0.0.0
Authentication Port:	1812
Accounting Port:	1813
Radius Secret Key:	private
IEEE802.1X Key Rotation:	600
IEEE802.1X Key Length:	64 bit
MAC ACL:	□ Enabled
Policy:	Allow

Fig. 2.8 IEEE802.1X (Access Point/Access Point WDS/ Repeater WDS)

This option apply to the following modes only, when WPA EAP or IEEE802.1x . **Access Point, Access Point WDS, Repeater WDS** modes.

Primary Radius Server IP

Enter the Primary Radius Server IP that Access Point will use to query server.

Secondary Radius Server IP

Enter the Secondary Radius Server IP that Access Point will use to query the server.

Authentication Port

Enter the Radius Server Authentication Port number to use. Default is 1812.

Accounting Port

Enter Radius server Accounting Port to use. Default is 1813.

Radius Secret Key

Enter Radius server Secret Key that Access Point to use to authenticate itself with radius server.

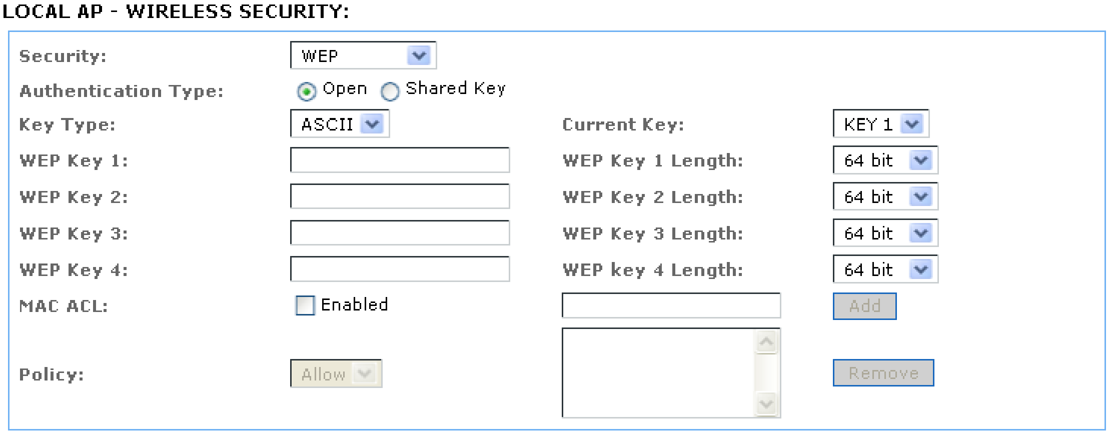
IEEE802.1x Key Rotation

Enter time in seconds. After time expired will initiate key rotation in authentication process for higher security.

IEEE802.1x Key Length

This is the key length of the initial seed key. Select 64 or 128bit.

WEP



LOCAL AP - WIRELESS SECURITY:

Security:	WEP		
Authentication Type:	● Open ○ Shared Key		
Key Type:	ASCII	Current Key:	KEY 1
WEP Key 1:		WEP Key 1 Length:	64 bit
WEP Key 2:		WEP Key 2 Length:	64 bit
WEP Key 3:		WEP Key 3 Length:	64 bit
WEP Key 4:		WEP key 4 Length:	64 bit
MAC ACL:	□ Enabled		Add
Policy:	Allow		Remove

Fig 2.6 WEP

The operation of the Keys is the same for ALL the modes.

**** Note: Operating with WEP security will limit AP to maximum wireless link speed of 54Mbps only.**

Authentication Type:

Open Authentication – (Default) No authentication. Recommend to use this standard option over shared authentication.

Shared Authentication – May not be compatible with all Access Point. Not recommended.

Key Type:

HEX or **ASCII** option specifies the character format for the WEP key if WEP security method is used.

Current Key:

Specify the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used.

WEP Key:

WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used.

WEP Key Length:

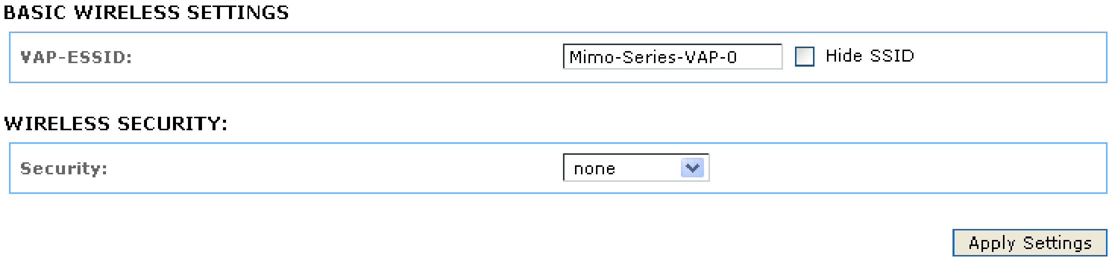
64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The 128-bit option will provide higher level of security.

For **64-bi**t – specify WEP key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.

For **128-bit** – specify WEP key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Virtual Access Point (VAP)

Virtual AP (VAP) implements mSSID (Multi-SSID) whereby a single wireless card can be setup with up to 3 virtual SSID of BSSID connections in the VAP setup page. Each VAP can be set with different security authentication mode.



BASIC WIRELESS SETTINGS

VAP-ESSID: Mimo-Series-VAP-0 □ Hide SSID

WIRELESS SECURITY:

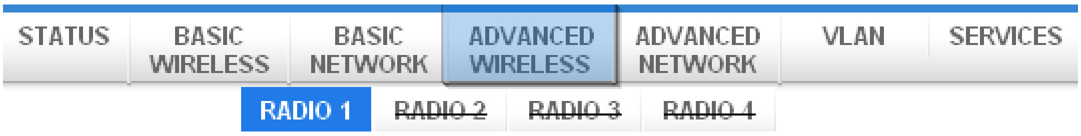
Security: none

Fig 2.11 Virtual AP (Only Available in Access Point/ Access Point WDS Mode)

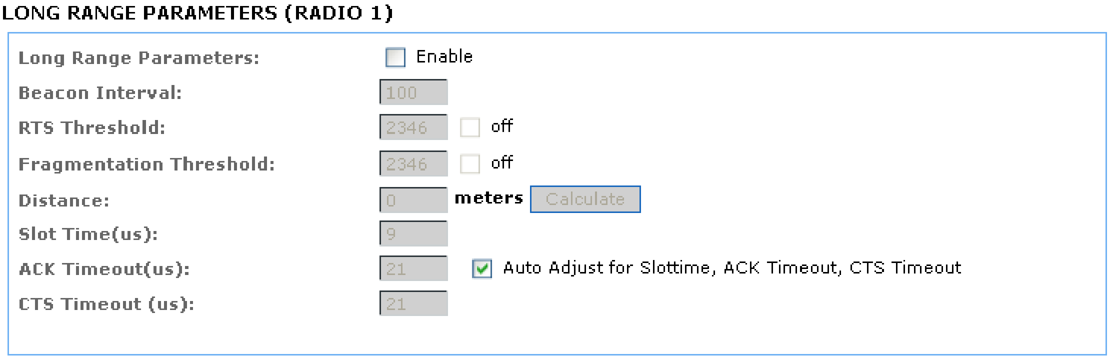
All VAPs are created from the same radio they all share the same wireless channel, country code, channel spectrum width and transmit power.

*** Note: Security options like IEEE802.1x and WPA-EAP uses radius server for authentication and accounting. You may not use different secret key for each VAP. Or you should configure only for one SSID with radius authentication.**

Advance Wireless Tab

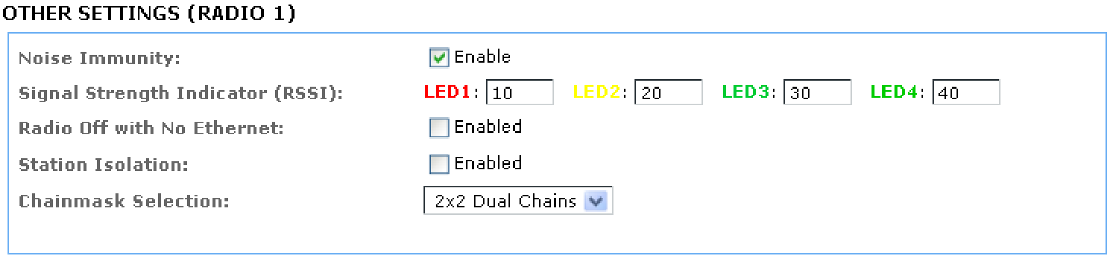


Click **Advanced Wireless** tab from menu and select **RADIO 1** to open the page below.



LONG RANGE PARAMETERS (RADIO 1)

Long Range Parameters:	□ Enable
Beacon Interval:	100
RTS Threshold:	2346 □ off
Fragmentation Threshold:	2346 □ off
Distance:	0 **meters** Calculate
Slot Time(us):	9
ACK Timeout(us):	21 ☑ Auto Adjust for Slottime, ACK Timeout, CTS Timeout
CTS Timeout (us):	21



OTHER SETTINGS (RADIO 1)

Noise Immunity:	☑ Enable
Signal Strength Indicator (RSSI):	LED1: 10 LED2: 20 LED3: 30 LED4: 40
Radio Off with No Ethernet:	□ Enabled
Station Isolation:	□ Enabled
Chainmask Selection:	2x2 Dual Chains

Long Range Parameters Setup

Advanced wireless page let you setup outdoor long distant connection parameters.

Long Range Parameters:

Check to enable parameters.

Beacon Interval: (default is 100 ms)

Define the time interval (in millisecond) the beacon to broadcast.

Recommend to use default.

RTS Threshold: (Default is **OFF**)

Fragmentation Threshold: (Default is **OFF**)

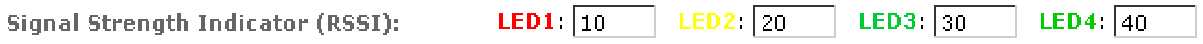
Distance:

Enter the distant in meters the device is to connect with the opposite device. Then click Calculate. The close approximate values for Slot Time, ACK Timeout, and CTS Timeout will be calculated. Fine tuning can be further adjusted for the best environment conditions to achieve best performance and better link reliability.

Noise Immunity:

Check to enable. When enabled, it automatically adjusts the signal/noise level for best performance. In low noise environment it is recommended to turn off this function.

Signal Strength Indicator (RSSI):



Signal Strength Indicator (RSSI): LED1: 10 LED2: 20 LED3: 30 LED4: 40

The default values are LED1-Red (10), LED2-Yellow (20), LED3-Green (40)
Each LEDs when turn on indicates the RSSI signal strength has hit over the value.
e.g. When LED1 and LED2 light up it indicate the RSSI is greater than 20.
When all 4 LEDs light up it indicate RSSI is greater than 40.
For long distant installation when signal strength expected to be about 20-30, the values can be adjusted to display over this new range.
e.g. the LEDs values can be adjusted as follows:

LED1 (RSSI value=7)
LED2 (RSSI value=15)
LED3 (RSSI value=22)
LED4 (RSSI value=27)

Radio Off with No Ethernet:

When checked, automatically stop wireless broadcast when Ethernet link down.

Station Isolation:

When checked, prevent wireless clients on same AP from discovering other clients.

Chainmask Selection:

Available selections are: a) **1x1 Left Chain**, b) **1x1 right Chain** and c) **2x2 Dual Chain**

Selecting **1x1 Left Chain** will forced radio card to operate with 1transmit and 1 receive stream and both transmit /receive on the left port of radio card only.

Selecting **1x1 Right Chain** will forced radio card to operate with 1 transmit and 1 receive stream and both transmit /receive on the right port of radio card only.

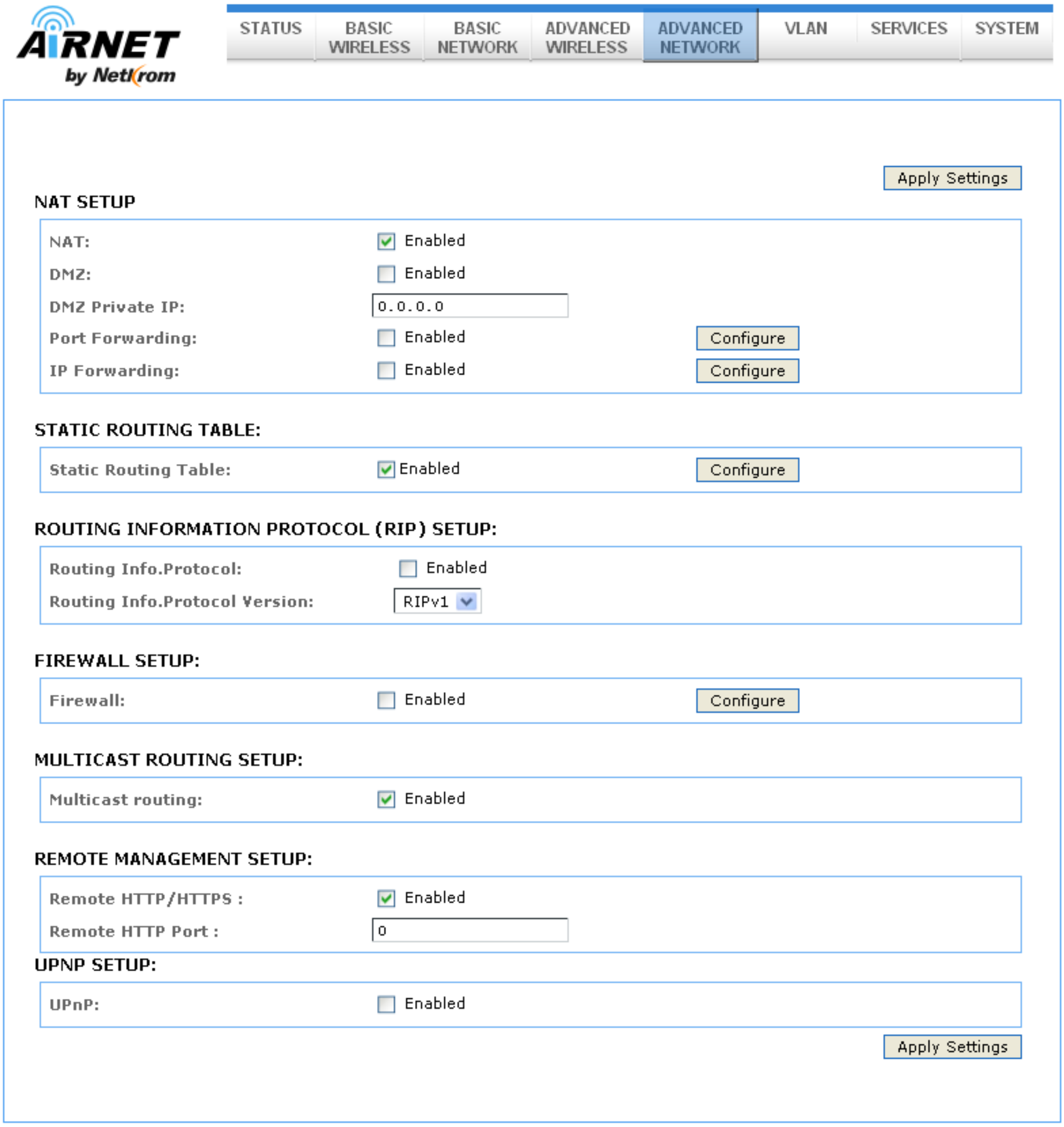
Selecting **2x2 Dual Chain** (default) will enable radio card to operate with 2 transmit and 2 receive streams and automatically transmit /receive on any of the 2 radio card ports.

Advanced Network Tab

Click **Advanced Network** tab from menu to open the page below.

***Note:** This tab will not open when the device is in Bridge node.

To open page, first enable Router mode in Basic Network (***We recommend to use first Station Mode, set an Static IP on WAN interface, and set a Remote Management Port, before going directly to Router mode. If you don't follow these steps you will lose control over the radio configuration!!!***)



NAT SETUP

NAT: ☑ Enabled

DMZ: □ Enabled

DMZ Private IP: 0.0.0.0

Port Forwarding: □ Enabled Configure

IP Forwarding: □ Enabled Configure

STATIC ROUTING TABLE:

Static Routing Table: ☑ Enabled Configure

ROUTING INFORMATION PROTOCOL (RIP) SETUP:

Routing Info.Protocol: □ Enabled

Routing Info.Protocol Version: RIPv1

FIREWALL SETUP:

Firewall: □ Enabled Configure

MULTICAST ROUTING SETUP:

Multicast routing: ☑ Enabled

REMOTE MANAGEMENT SETUP:

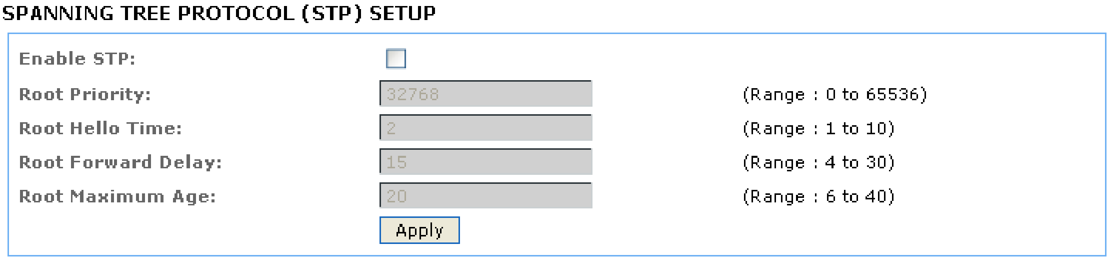
Remote HTTP/HTTPS : ☑ Enabled

Remote HTTP Port : 0

UPNP SETUP:

UPnP: □ Enabled

Spanning Tree Setup



SPANNING TREE PROTOCOL (STP) SETUP

Enable STP:	□	
Root Priority:	32768	(Range : 0 to 65536)
Root Hello Time:	2	(Range : 1 to 10)
Root Forward Delay:	15	(Range : 4 to 30)
Root Maximum Age:	20	(Range : 6 to 40)
	Apply	

Spanning Tree Protocol: Default is **disabled**. Check on box to enable.

Root Priority: Default value is 32768. Smaller value has higher priority.

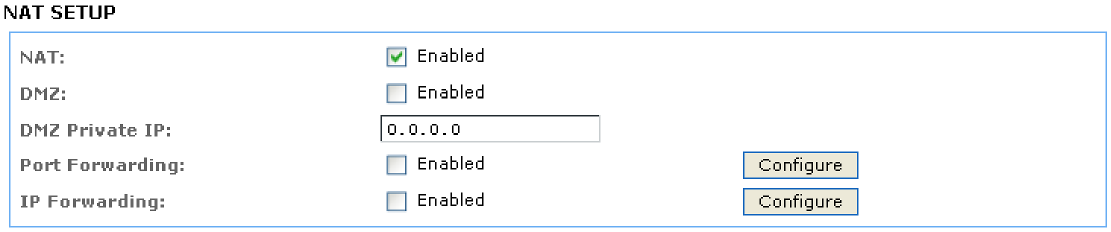
Root Hello Time: Default time is 2 seconds.

Root Forward Delay: Default is 15 seconds

Root Maximum Age: Default is 20 seconds

Changing to lower time can caused high overheads to the network.

NAT Setup



NAT SETUP

NAT:	☑ Enabled	
DMZ:	□ Enabled	
DMZ Private IP:	0.0.0.0	
Port Forwarding:	□ Enabled	Configure
IP Forwarding:	□ Enabled	Configure

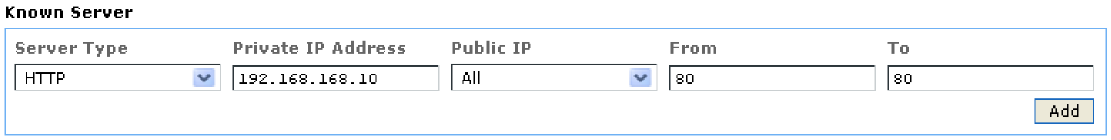
NAT: Enabled when in Router mode. Disabled when in Bridge mode.

DMZ: Default is disabled. Check on box to enable.

DMZ IP Address: Input IP address of the local PC to receive the DMZ packets.

Port Forwarding: Default is disabled. Check on box to enable.

For configuration refer to Appendix section.



Known Server

Server Type	Private IP Address	Public IP	From	To
HTTP	192.168.168.10	All	80	80
				Add

Adding an entry from Known Server

Add entry from this box and select an application the list.

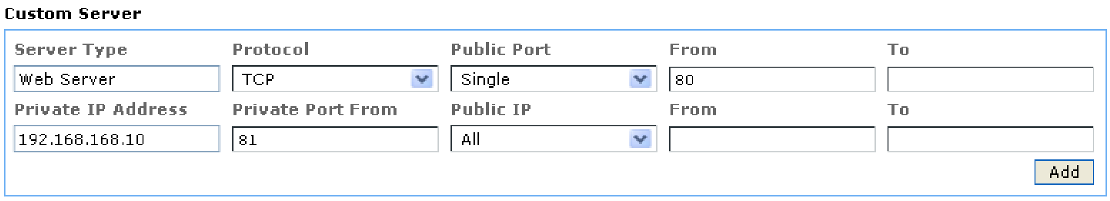
Server Type: click to select the application you want to add.

Private IP Address: Enter the local IP of the PC running the application

Public IP Address: If the application to for any people on the internet to access then select the default, **All**.

If only specific IP, select **Single** and enter the IP address.

If only specific range of IP, select **Range** and enter IP address range.



Custom Server

Server Type	Protocol	Public Port	From	To
Web Server	TCP	Single	80	
Private IP Address	Private Port From	Public IP	From	To
192.168.168.10	81	All		

Adding an entry from Custom Server

Entry from Custom Server box lets you enter the other port number service for an application and new applications.

Custom Server also lets you enter a different public and private port service

Server Type: Enter a brief name for the application. This info helps you track the application for that port number you set.

Protocol: Select TCP or UDP the application use.

Public Port: select Single or Range of ports application use.

From: if single port, enter this box only. If port range, enter starting port number here.

To: if single port, leave blank. if port range enter, enter last port number here.

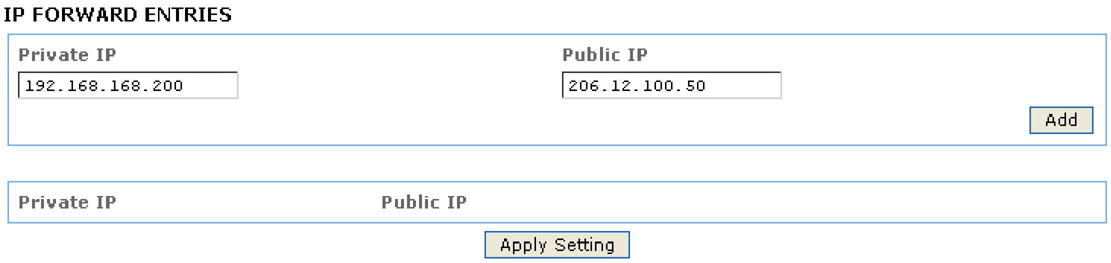
Private IP Address: Enter the local IP of the PC running the application

Private Port From: If single port, enter same public port number or new port number. If port range, enter only the starting port number.

Public IP Address: If the application is to access by any people on the internet, then select the default, **All**.

If only specific IP, select **Single** and enter the IP address.

If only specific range of IP, select **Range** and enter IP address range.



IP FORWARD ENTRIES

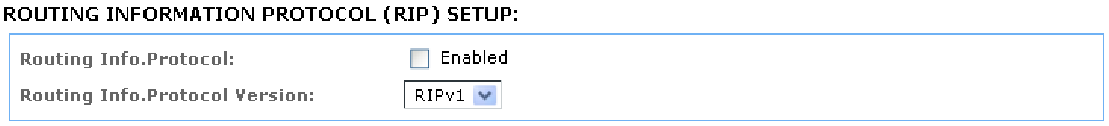
Private IP	Public IP
192.168.168.200	206.12.100.50

IP Forwarding: Default is disabled. Check on box to enable. For configuration refer to Appendix section.

Private IP: enter the local IP address to receive forward packet by the public IP

Public IP: enter the public IP address when access will forward all packet to the local IP

Click Add to add to list.



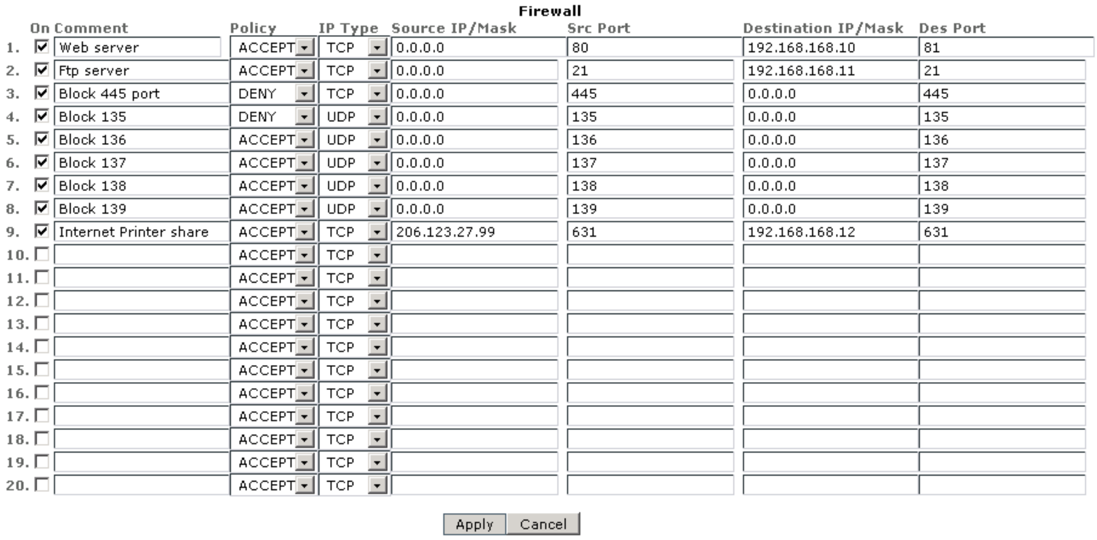
ROUTING INFORMATION PROTOCOL (RIP) SETUP:

Routing Info.Protocol:	□ Enabled
Routing Info.Protocol Version:	RIPv1

Routing Information Protocol: Default is disabled. Check on box to enable. For configuration refer to Appendix section.

Router Info Protocol version: select RIPv1 or RIPv2

Firewall Setup



Firewall

	On	Comment	Policy	IP Type	Source IP/Mask	Src Port	Destination IP/Mask	Des Port
1.	☑	Web server	ACCEPT	TCP	0.0.0.0	80	192.168.168.10	81
2.	☑	Ftp server	ACCEPT	TCP	0.0.0.0	21	192.168.168.11	21
3.	☑	Block 445 port	DENY	TCP	0.0.0.0	445	0.0.0.0	445
4.	☑	Block 135	DENY	UDP	0.0.0.0	135	0.0.0.0	135
5.	☑	Block 136	ACCEPT	UDP	0.0.0.0	136	0.0.0.0	136
6.	☑	Block 137	ACCEPT	UDP	0.0.0.0	137	0.0.0.0	137
7.	☑	Block 138	ACCEPT	UDP	0.0.0.0	138	0.0.0.0	138
8.	☑	Block 139	ACCEPT	UDP	0.0.0.0	139	0.0.0.0	139
9.	☑	Internet Printer share	ACCEPT	TCP	206.123.27.99	631	192.168.168.12	631
10.	□		ACCEPT	TCP				
11.	□		ACCEPT	TCP				
12.	□		ACCEPT	TCP				
13.	□		ACCEPT	TCP				
14.	□		ACCEPT	TCP				
15.	□		ACCEPT	TCP				
16.	□		ACCEPT	TCP				
17.	□		ACCEPT	TCP				
18.	□		ACCEPT	TCP				
19.	□		ACCEPT	TCP				
20.	□		ACCEPT	TCP				

Firewall Setup: Default is disabled. Check on box to enable.
For configuration refer to Appendix section.

Comment: enter a brief name for the service.

Policy: select Accept or Deny for the apply rule

IP Type: select ICMP, TCP, and UDP packet type to check

Source IP/Mask: enter the source IP address and Netmask
Is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;

Src Port: enter the source port number in rule check
Is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets.

Destination IP/Mask: enter the destination IP and Netmask
Is the Destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;

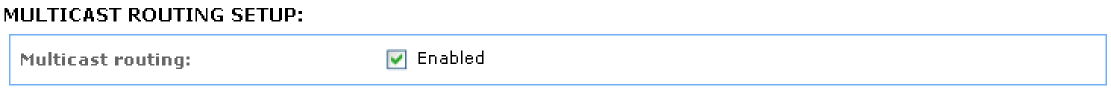
Des Port: enter the destination port in rule check
Is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to

.

Click **Apply** to the rule or **Cancel** to clear the rule set.

Multicast Routing Setup

Disabling this option disallows video streaming over the Internet. Click **Apply** to complete setup.



MULTICAST ROUTING SETUP:

Multicast routing: ☑ Enabled

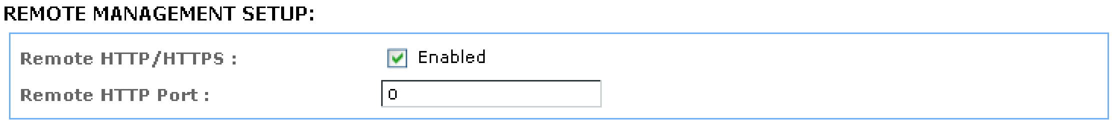
Remote Management Setup

To enable Remote Management, set **Remote Http Port** to an unused port number. It is recommended that you avoid using port number 80 as it is blocked by some ISPs.

To disable Remote Management, set **Remote Http Port** to 0

In Router mode with Access Point Mode, **Remote Management** is disabled and the Ethernet port becomes a WAN port. To continue using it, enter the Remote Management with port 88 for example.

Example: For WAN IP 100.100.100.1 use http://100.100.100.1:88



REMOTE MANAGEMENT SETUP:

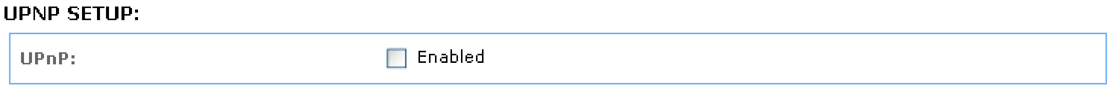
Remote HTTP/HTTPS : ☑ Enabled

Remote HTTP Port : 0

UPNP:

Default is disabled. Check on box to enabled. When enabled, client PC running Microsoft UPnP services can automatically open certain specific port required by the PC application in the router. For security reason this service should not be open.

Recommend to setup manually open all port service through **Port Forwarding** service.

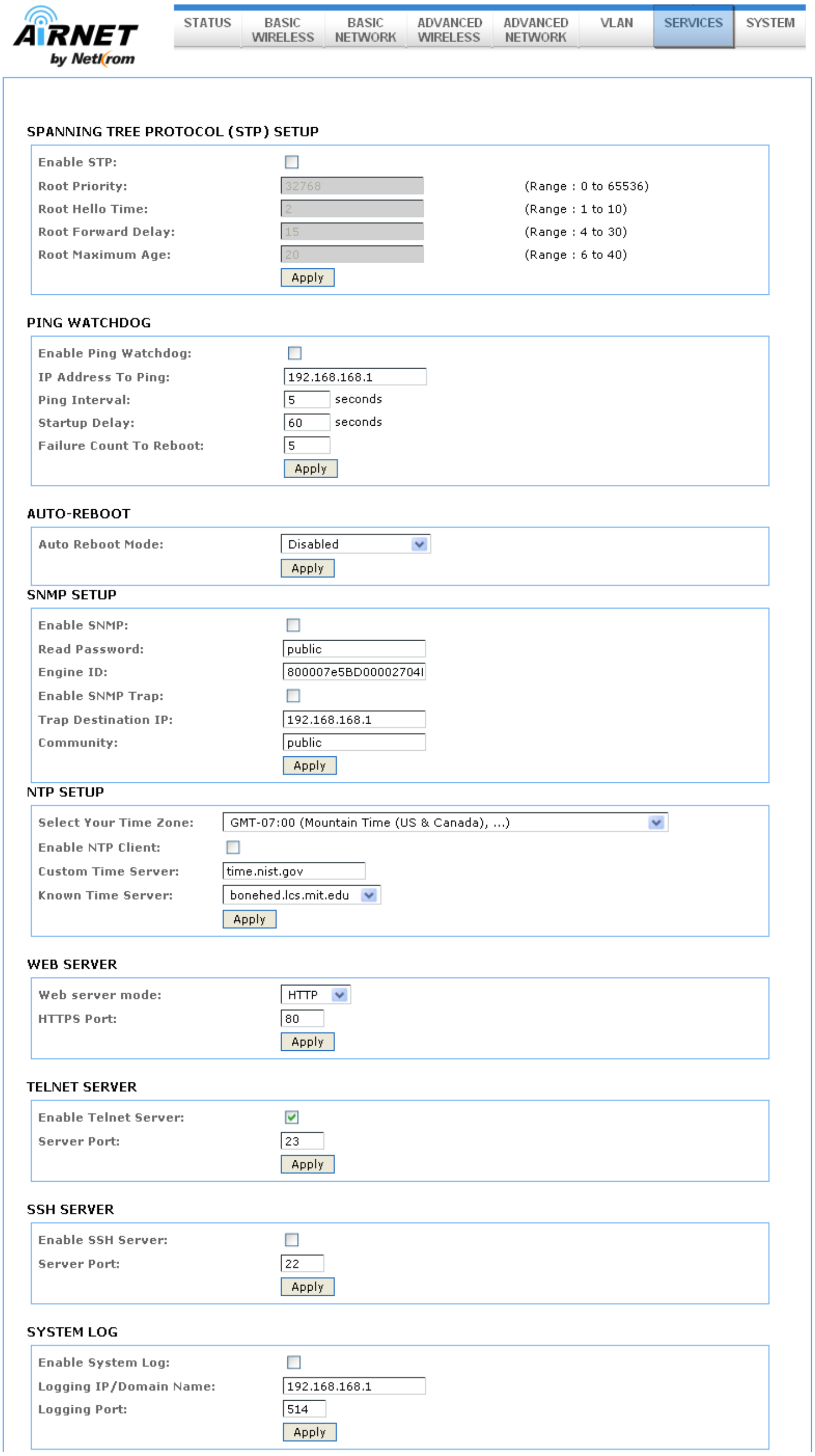


UPNP SETUP:

UPnP: □ Enabled

Services Tab

Click **Services** tab from menu to open the page below.
Services section provides varieties of useful and enhanced functions to help assist device operations.



SPANNING TREE PROTOCOL (STP) SETUP

Enable STP:	□	
Root Priority:	32768	(Range : 0 to 65536)
Root Hello Time:	2	(Range : 1 to 10)
Root Forward Delay:	15	(Range : 4 to 30)
Root Maximum Age:	20	(Range : 6 to 40)
	Apply	

PING WATCHDOG

Enable Ping Watchdog:	□
IP Address To Ping:	192.168.168.1
Ping Interval:	5 seconds
Startup Delay:	60 seconds
Failure Count To Reboot:	5
	Apply

AUTO-REBOOT

Auto Reboot Mode:	Disabled
	Apply

SNMP SETUP

Enable SNMP:	□
Read Password:	public
Engine ID:	800007e5BD00002704I
Enable SNMP Trap:	□
Trap Destination IP:	192.168.168.1
Community:	public
	Apply

NTP SETUP

Select Your Time Zone:	GMT-07:00 (Mountain Time (US & Canada), ...)
Enable NTP Client:	□
Custom Time Server:	time.nist.gov
Known Time Server:	bonehed.lcs.mit.edu
	Apply

WEB SERVER

Web server mode:	HTTP
HTTPS Port:	80
	Apply

TELNET SERVER

Enable Telnet Server:	☑
Server Port:	23
	Apply

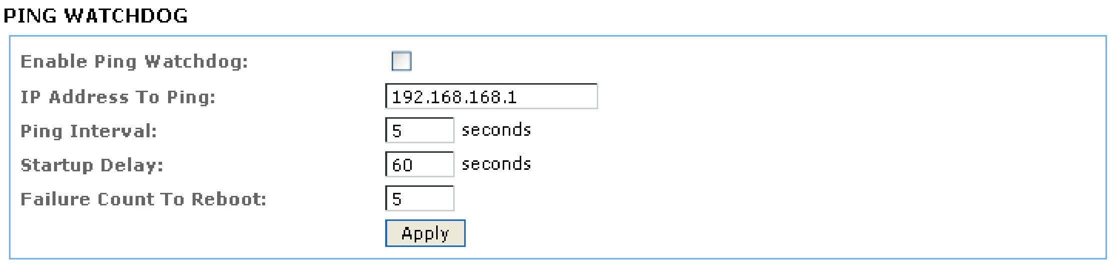
SSH SERVER

Enable SSH Server:	□
Server Port:	22
	Apply

SYSTEM LOG

Enable System Log:	□
Logging IP/Domain Name:	192.168.168.1
Logging Port:	514
	Apply

Ping Watchdog



PING WATCHDOG

Enable Ping Watchdog: □

IP Address To Ping: 192.168.168.1

Ping Interval: 5 seconds

Startup Delay: 60 seconds

Failure Count To Reboot: 5

Enable Ping Watchdog: Default is disabled. Check on box to enable.

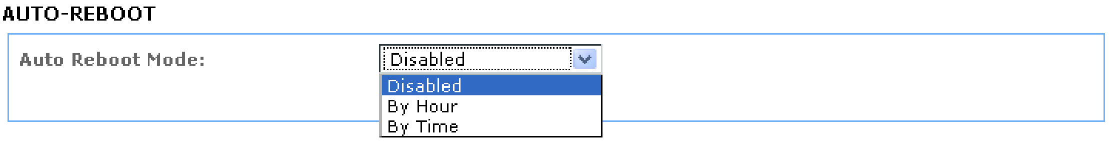
IP Address To Ping: Target IP address do ping test monitor.

Ping Interval: Default is 5 seconds (minimum). This is Ping test duration.

Startup Delay: Default is 60 seconds (minimum).
One time delay after device startup.

Failed Count to Reboot: Default is 5. This is the number of ping failure count before device kick in the reboot process.

Auto-Reboot



AUTO-REBOOT

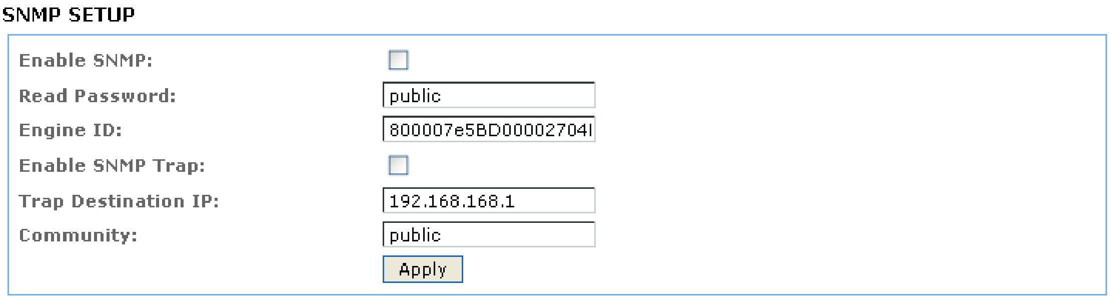
Auto Reboot Mode: Disabled

Auto-Reboot Mode: Default is disabled. Select By Hour or By Time check.
This mode lets you preset a timer to automatically force a reboot.
Timer can in fixed number of hours or at a specified time of day.

By Hour: Enter the number of hours device need to run before kick start reboot process.

By Time: Enter the specific time of day in hh:mm (24-hour format) to kick start reboots process.

SNMP Setup



SNMP SETUP

Enable SNMP: □

Read Password: public

Engine ID: 800007e5BD00002704I

Enable SNMP Trap: □

Trap Destination IP: 192.168.168.1

Community: public

Enable SNMP: Default is disabled. Check on box to enable.

Read Only Password: Password to query device.

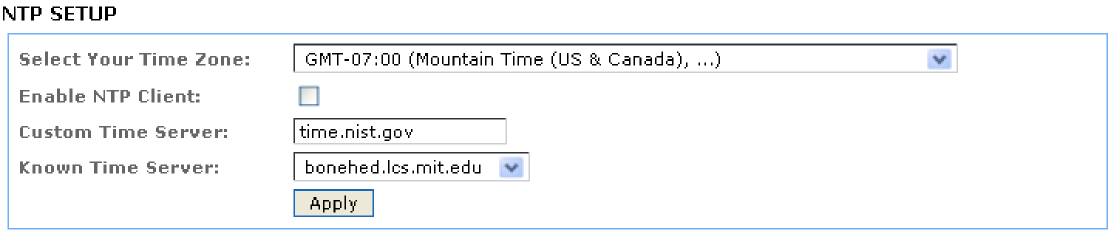
Engine ID: Default is 800007e5BD00002704D000007c

Enable SNMP Trap: Default is disabled. Check on box to enable.

Trap Destination IP: Enter the IP to send the info when trap is triggered.

Community: Enter the SNMP community string.

NTP Setup



NTP SETUP

Select Your Time Zone: GMT-07:00 (Mountain Time (US & Canada), ...)

Enable NTP Client: □

Custom Time Server: time.nist.gov

Known Time Server: bonehed.lcs.mit.edu

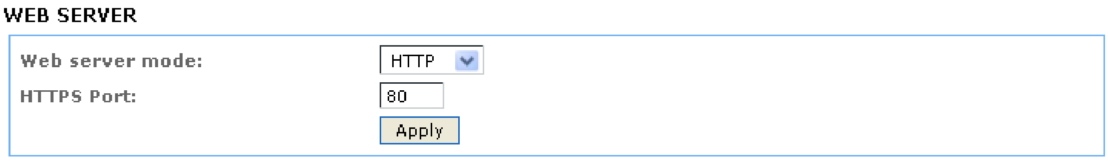
Enable NTP Client: Default is disabled. Check on box to enable.

Select Your Time Zone: Select from list the country you reside.

Custom Time Server: Default is “time.nist.gov“ Enter preferred time server domain or IP

Known Time Server: You can also select one from this list as your new time server.

Web HTTP Security



WEB SERVER

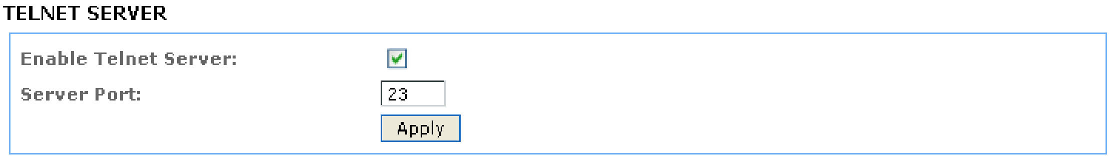
Web server mode: HTTP

HTTPS Port: 80

Web Server Mode: Default is HTTP. Option is HTTP and HTTPs

HTTP(s) Port: Default is 80 for HTTP and 413 for HTTPs.
Enter a new preferred port number.

Telnet Access Setup


TELNET SERVER

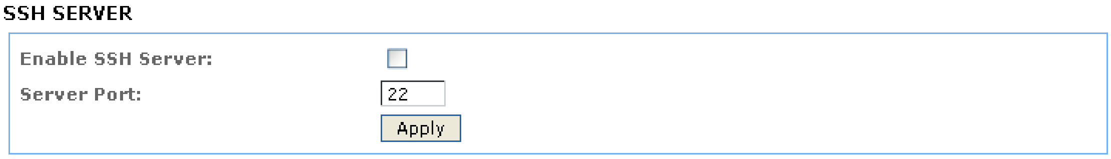
Enable Telnet Server: ☑

Server Port: 23

Enable Telnet Server: Default is enabled. Remove check on box to disable.

Server Port: Default is 23. Enter new preferred port number.

SSH Access Setup


SSH SERVER

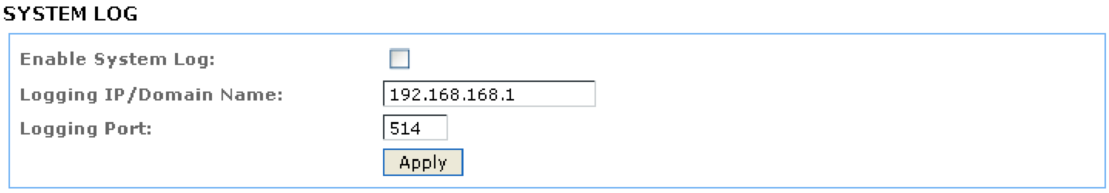
Enable SSH Server: □

Server Port: 22

Enable SSH Server: Default is disabled. Check on box to enable.

Server Port: Default is 22. Enter new preferred port number.

System Log Setup


SYSTEM LOG

Enable System Log: □

Logging IP/Domain Name: 192.168.168.1

Logging Port: 514

Enable System Logging: Default is disabled. Check on box to enable.

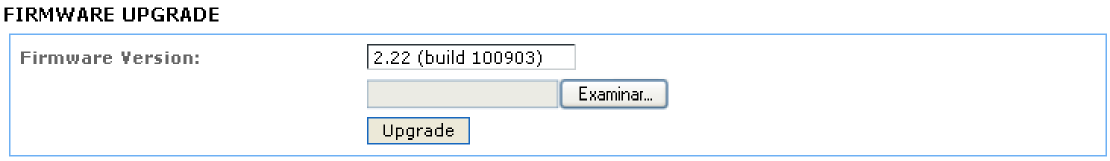
Logging IP /Domain Name: Enter destination IP address of device to receive log.

Logging Port: Default is 514. Enter the new preferred port number.

System Tab

The System Page contains Administrative options. This page enables administrator to customize, reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator's credentials.

Firmware Upgrade



FIRMWARE UPGRADE

Firmware Version: 2.22 (build 100903)

Use this section to find out current software version and update the device with the new firmware. The device firmware update is compatible with all configuration settings. System configurations are preserved while the device is updated with a new firmware version.

Firmware version: displays the version of the current firmware of the device system.

Upgrade: button opens the Firmware Upload window if activated.

Current Firmware: displays the version of the device firmware which is currently operating.

Firmware File: activate Browse button to navigate to and select the new firmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after Upload button is activated.

Close this window – button cancels the new firmware upload process if activated.

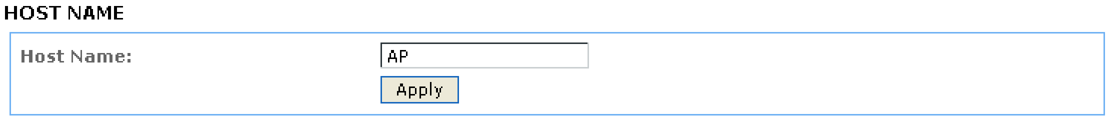
Upgrade button should be activated in order to proceed with firmware upgrade routine (new firmware image should be uploaded into the system first). Please be patient, as the firmware upgrade routine can take 3-7 minutes. The based device will be un-accessible until the firmware upgrade routine is completed.

Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!

It is highly recommended to backup the system configuration and the Support Info file before uploading the new configuration.

Close this window – button closes the firmware upgrade window if activated. This action will not cancel the firmware upgrade process.

Host Name



HOST NAME

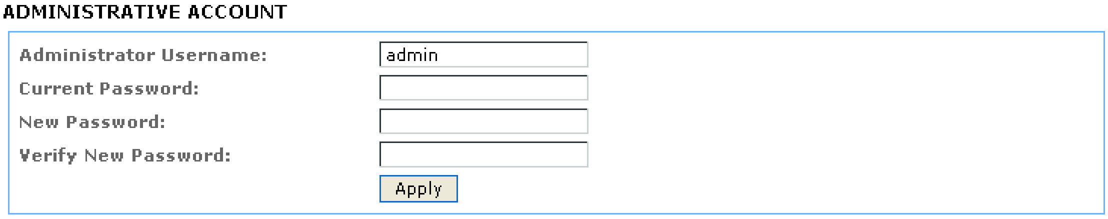
Host Name: AP

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations. Host Name will be represented in popular Router Operating Systems registration screens and discovery tools.

Host Name: specifies the system identity.

Change button saves the Host Name if activated.

Administrative and Read-only Account



ADMINISTRATIVE ACCOUNT

Administrator Username: admin

Current Password:

New Password:

Verify New Password:

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup:

Administrator Username: specifies the name of the system user.

Current Password: administrator is required to enter a current password. It is required for Password or Administrator Username change routine.

Default administrator login credentials:

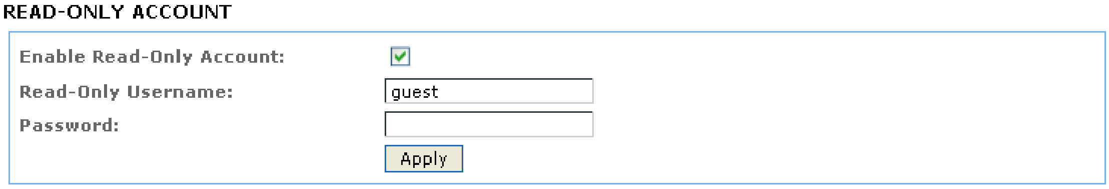
- User Name: **admin**
- Password: **password**

New Password: new password used for administrator authentication should be specified.

Verify Password: new password should be re-entered to verify its accuracy.

Click Change button to save the changes.

Enable Read-Only Account



READ-ONLY ACCOUNT

Enable Read-Only Account: ☑

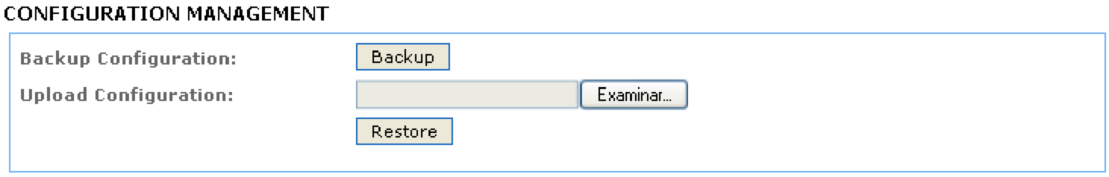
Read-Only Username: guest

Password:

Read-Only Username

Password: new password used for read-only administrator authentication should be specified.

Configuration Management



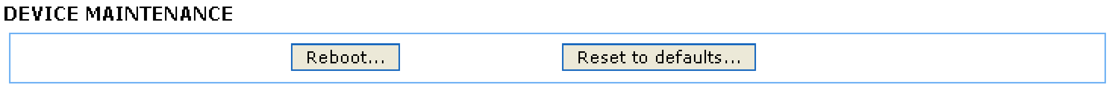
CONFIGURATION MANAGEMENT

Backup Configuration:

Upload Configuration:

Backup Configuration: click Download button to export the current configuration to a file.
Upload Configuration: click Browse button to navigate to and select the new configuration file or specify the full path to the configuration file location.
Activating the Upload button will transfer new configuration file to the system.
New configuration will be effective after the Apply button is activated and system reboot cycle is completed. Previous system configuration is deleted after Apply button is activated. It is highly recommended to backup the system configuration before uploading the new configuration.
Use only configuration backups of the same type device - configuration backed up from PowerStation2 suits only PowerStation2, but not LiteStation2 or LiteStation5! Behavior may be unpredictable when mixing configurations from different type devices.

Device Maintenance



DEVICE MAINTENANCE

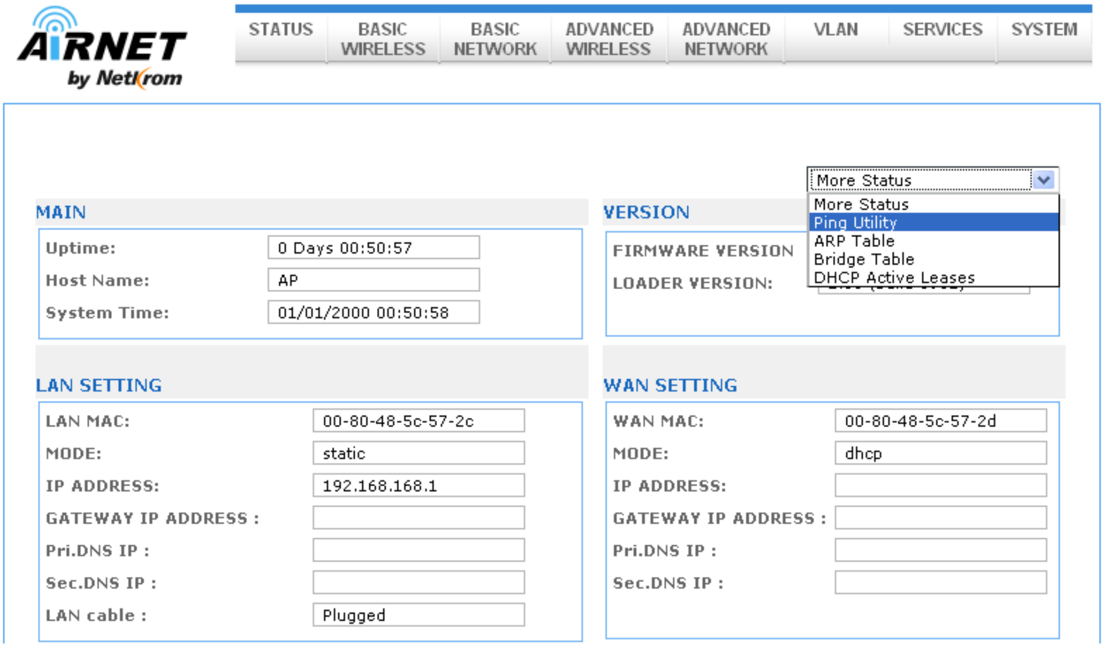
The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, generating of the support information report.

Reboot: activate Reboot control in order to initiate full reboot cycle of the device. Reboot effect is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

Reset to Defaults: activate Reset to Defaults control in order to initiate reset the device to factory defaults routine. Reset routine initiates system Reboot process (similar to the power off - power on cycle). The running system configuration will be deleted and the default system configuration (all the system settings with no exception) will be set.

After the **Reset to Defaults** routine is completed, the device system will return to the default IP configuration (192.168.168.1/255.255.255.0) and will start operating in Station-Bridge mode. It is highly recommended to backup the system configuration before the Reset to Defaults is initiated.

Status Page



MAIN

Uptime:	0 Days 00:50:57
Host Name:	AP
System Time:	01/01/2000 00:50:58

VERSION

FIRMWARE VERSION	
LOADER VERSION:	[illegible]

LAN SETTING

LAN MAC:	00-80-48-5c-57-2c
MODE:	static
IP ADDRESS:	192.168.168.1
GATEWAY IP ADDRESS :	
Pri.DNS IP :	
Sec.DNS IP :	
LAN cable :	Plugged

WAN SETTING

WAN MAC:	00-80-48-5c-57-2d
MODE:	dhcp
IP ADDRESS:	
GATEWAY IP ADDRESS :	
Pri.DNS IP :	
Sec.DNS IP :	

The Status Page displays a summary of link status information, current values of basic configuration settings (depending on operating mode), network settings and traffic statistics of all the interfaces.

Status Reporting

Main

Uptime: displays device up time since boot up. The time is expressed in days, hours, minutes and seconds.

Host Name: displays the assigned device host name (ID).

System Time: display device current date and time. Accurate system date and time is retrieved from the internet services using NTP (Network Time Protocol) if device is setup and connected to internet. Otherwise, the date and time update from device own inaccurate autonomous clock.

Version Firmware Version: displays current firmware version in operation.

Loader Version: displays current loader version of the device.

LAN Setting

LAN MAC: displays the MAC address of the device LAN (Ethernet) interface.
LAN Mode: displays the mode used, either static or DHCP client.
LAN IP Address: displays the current IP address of the LAN (Ethernet) interface.
LAN Gateway IP Address: displays the IP address of the gateway used in LAN.
LAN Pri. DNS IP: displays the Primary DNS IP address of the LAN setting.
LAN Sec. DNS IP: displays the Secondary DNS IP address of the LAN setting.

WAN Setting

WAN MAC: displays the MAC address of the device WAN interface.
WAN Mode: displays the mode used, either DHCP, PPPoE or Static IP.
WAN IP Address: displays the current IP address of the WAN interface.
WAN Gateway IP Address: displays the IP address of the gateway used in WAN.
WAN Pri. DNS IP: displays the Primary DNS IP address of the WAN setting.
WAN Sec. DNS IP: displays the Secondary DNS IP address of the WAN setting.

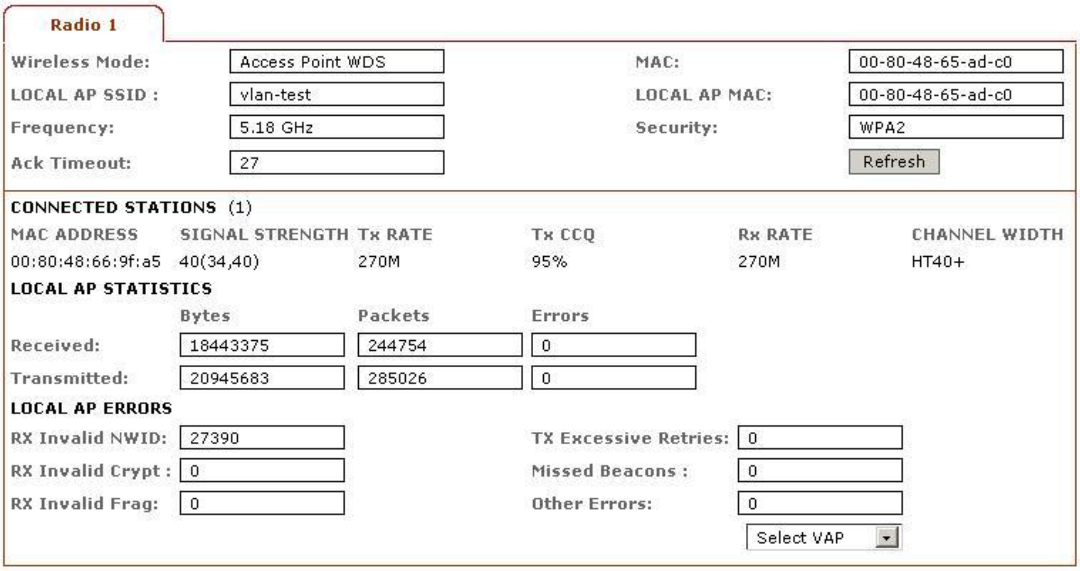
Radio

Wireless Mode: displays the current operating mode of the device.
Local AP SSID: displays the current SSID (Service Set Identifier) of device when operates in access point mode.
Frequency: displays current operating frequency running in device.
WLAN MAC: displays the MAC address or BSSID of the current active WLAN card running in device.
WLAN Local/Remote AP MAC: displays the MAC address of the WLAN card connected to it.
WLAN Security: display the current active security mode.

Clients Connection Status in AP Status Info

All clients connected to AP can be view from AP Status page.
Below is an example of a client connection status info.

Click Refresh to refresh client connection statistics and status page.



Radio 1

Wireless Mode:	Access Point WDS	MAC:	00-80-48-65-ad-c0
LOCAL AP SSID :	vlan-test	LOCAL AP MAC:	00-80-48-65-ad-c0
Frequency:	5.18 GHz	Security:	WPA2
Ack Timeout:	27		Refresh

CONNECTED STATIONS (1)

MAC ADDRESS	SIGNAL STRENGTH	Tx RATE	Tx CCQ	Rx RATE	CHANNEL WIDTH
00:80:48:66:9f:a5	40(34,40)	270M	95%	270M	HT40+

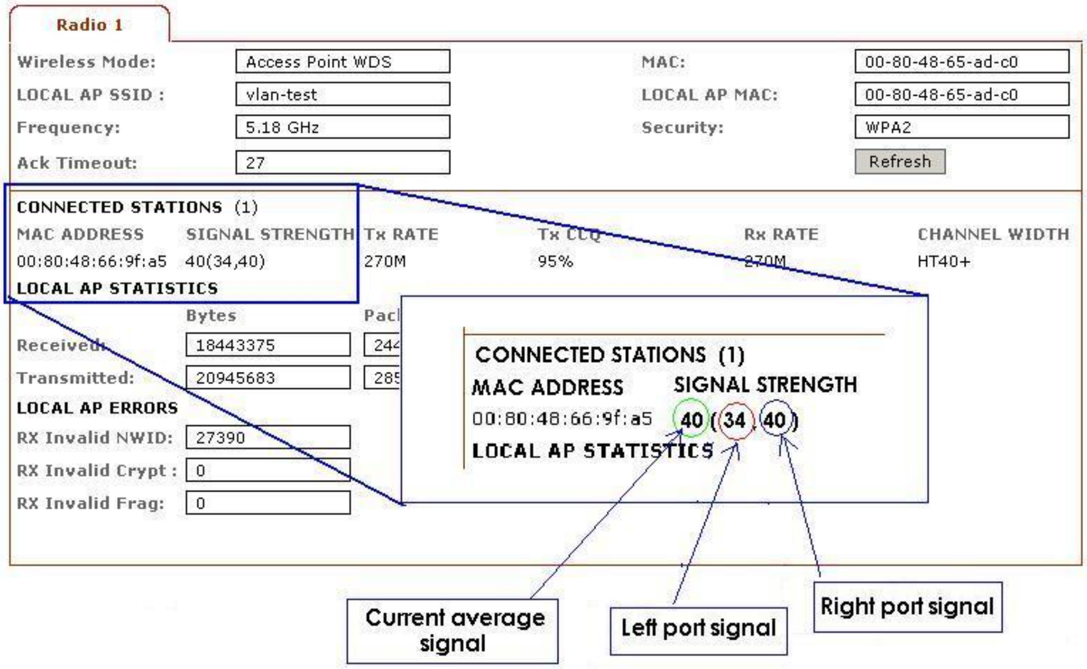
LOCAL AP STATISTICS

	Bytes	Packets	Errors
Received:	18443375	244754	0
Transmitted:	20945683	285026	0

LOCAL AP ERRORS

RX Invalid NWID:	27390	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

Select VAP



Radio 1

Wireless Mode:	Access Point WDS	MAC:	00-80-48-65-ad-c0
LOCAL AP SSID :	vlan-test	LOCAL AP MAC:	00-80-48-65-ad-c0
Frequency:	5.18 GHz	Security:	WPA2
Ack Timeout:	27		Refresh

CONNECTED STATIONS (1)

MAC ADDRESS	SIGNAL STRENGTH	Tx RATE	Tx CCQ	Rx RATE	CHANNEL WIDTH
00:80:48:66:9f:a5	40(34,40)	270M	95%	270M	HT40+

LOCAL AP STATISTICS

	Bytes	Pacl
Received:	18443375	244
Transmitted:	20945683	285

LOCAL AP ERRORS

RX Invalid NWID:	27390
RX Invalid Crypt :	0
RX Invalid Frag:	0

CONNECTED STATIONS (1)

MAC ADDRESS	SIGNAL STRENGTH
00:80:48:66:9f:a5	40 (34 , 40)

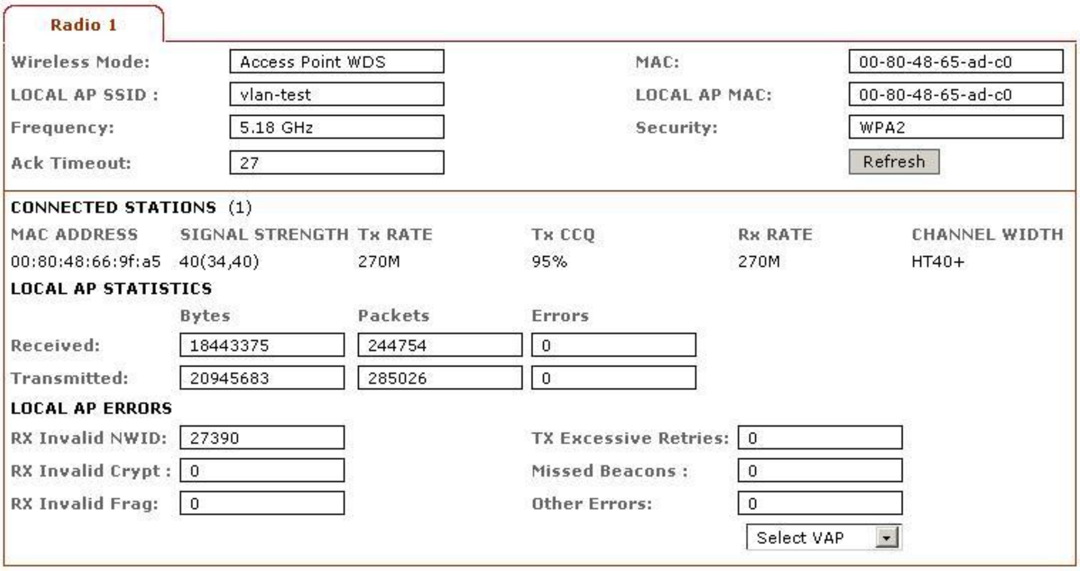
LOCAL AP STATISTICS

Signals strength at the left and right port of radio card can be view with more accurately while adjusting the antenna to get a more balanced reception.

Station Connection Info

Status Info

Click Refresh to refresh client connection statistics and status page.



Radio 1

Wireless Mode:	Access Point WDS	MAC:	00-80-48-65-ad-c0
LOCAL AP SSID :	vlan-test	LOCAL AP MAC:	00-80-48-65-ad-c0
Frequency:	5.18 GHz	Security:	WPA2
Ack Timeout:	27		Refresh

CONNECTED STATIONS (1)

MAC ADDRESS	SIGNAL STRENGTH	Tx RATE	Tx CCQ	Rx RATE	CHANNEL WIDTH
00:80:48:66:9f:a5	40(34,40)	270M	95%	270M	HT40+

LOCAL AP STATISTICS

	Bytes	Packets	Errors
Received:	18443375	244754	0
Transmitted:	20945683	285026	0

LOCAL AP ERRORS

RX Invalid NWID:	27390	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

WLAN Connected Status:

MAC Address: displays the MAC address of the current active WLAN card.

Signal Strength: displays the received wireless signal level of opposite connected device.

TX Rate and RX Rate: displays the current 802.11 data transmission (TX) and data reception (RX) rate while operating in Station mode. Typically, the higher the signal, the higher the data rate and consequently the higher the data throughput.

Channel Width:

20MHz – is the standard channel spectrum width (selected by default).

40MHz – the widest channel spectrum width required to connect to an 802.11a network which supports Static Turbo feature

WLAN Local AP Statistics:

Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;

WLAN Local AP Errors: section displays the counters of 802.11 specific errors which were registered on wireless interface:

Rx invalid NWID value represents the number of packets received with a different NWID or ESSID - packets which were destined for another access point. It can help to detect configuration problems or identify the adjacent wireless network existence on the same frequency. Value increase indicates AP channel is adjacent to many wireless networks.

Rx Invalid Crypt value represents the number of transmitted and received packets which were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid wireless security settings and encryption break attempts.

Rx Invalid Frag value represents the number of packets missed during transmission and reception. These packets were dropped due to re-assembling failure as some link layer fragments of the packet were lost.

Tx Excessive Retries value represents the number of packets which failed to be delivered to the destination. Undelivered packet are retransmitted a number of times before an error occurs.

Missed beacons value represents the number beacons (management packets sent at regular intervals by the Access Point) which were missed by the client. This can indicate that the wireless client is out of range.

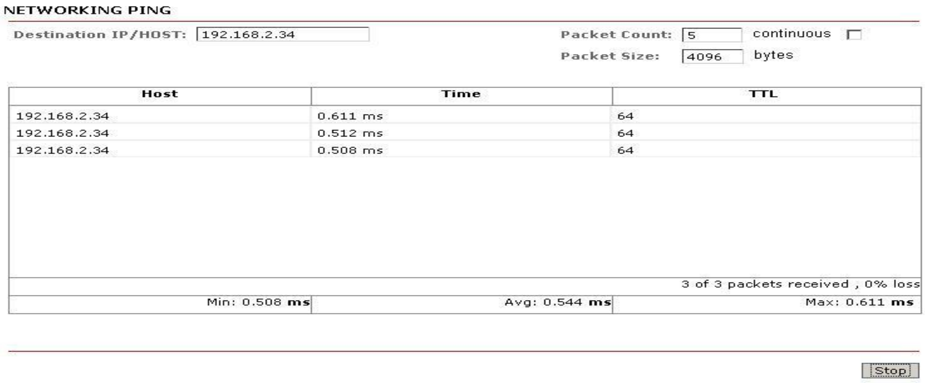
Other errors value represents the total number of transmitted and received packets that were lost or discarded for other reasons.

--

More Status

In More Status option contains some useful tools and additional status pages.

Ping Utility – a ping tool to test the connectivity between devices.



NETWORKING PING

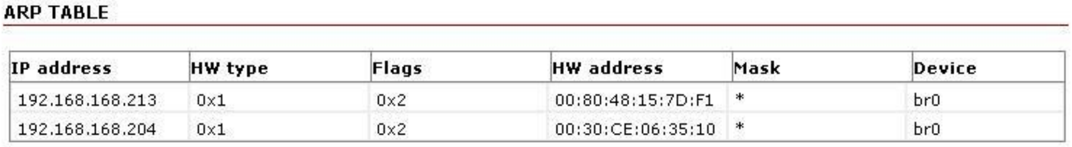
Destination IP/HOST: 192.168.2.34

Packet Count: 5 continuous □

Packet Size: 4096 bytes

Host	Time	TTL
192.168.2.34	0.611 ms	64
192.168.2.34	0.512 ms	64
192.168.2.34	0.508 ms	64
		3 of 3 packets received , 0% loss
Min: 0.508 **ms**	Avg: 0.544 **ms**	Max: 0.611 **ms**

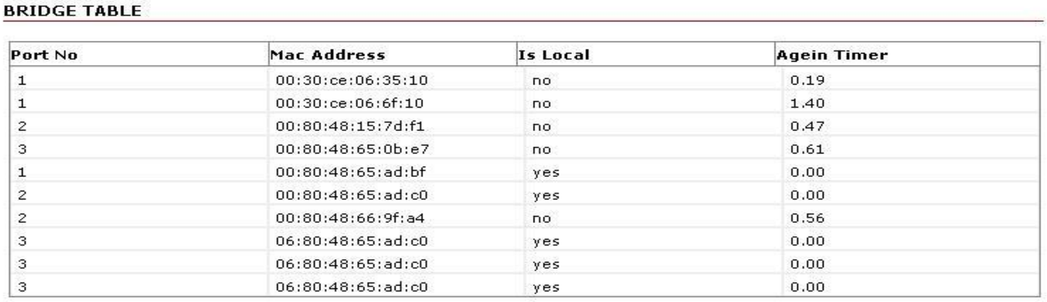
ARP Table display a list of MAC addresses of the connected devices



ARP TABLE

IP address	HW type	Flags	HW address	Mask	Device
192.168.168.213	0x1	0x2	00:80:48:15:7D:F1	*	br0
192.168.168.204	0x1	0x2	00:30:CE:06:35:10	*	br0

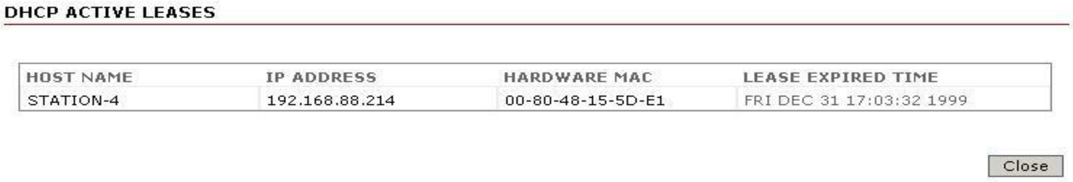
Bridge Table display a list the devices connect to the bridge interface



BRIDGE TABLE

Port No	Mac Address	Is Local	Agein Timer
1	00:30:ce:06:35:10	no	0.19
1	00:30:ce:06:6f:10	no	1.40
2	00:80:48:15:7d:f1	no	0.47
3	00:80:48:65:0b:e7	no	0.61
1	00:80:48:65:ad:bf	yes	0.00
2	00:80:48:65:ad:c0	yes	0.00
2	00:80:48:66:9f:a4	no	0.56
3	06:80:48:65:ad:c0	yes	0.00
3	06:80:48:65:ad:c0	yes	0.00
3	06:80:48:65:ad:c0	yes	0.00

DHCP Active Lease Table display a list of IPs addresses leased to all computers.



DHCP ACTIVE LEASES

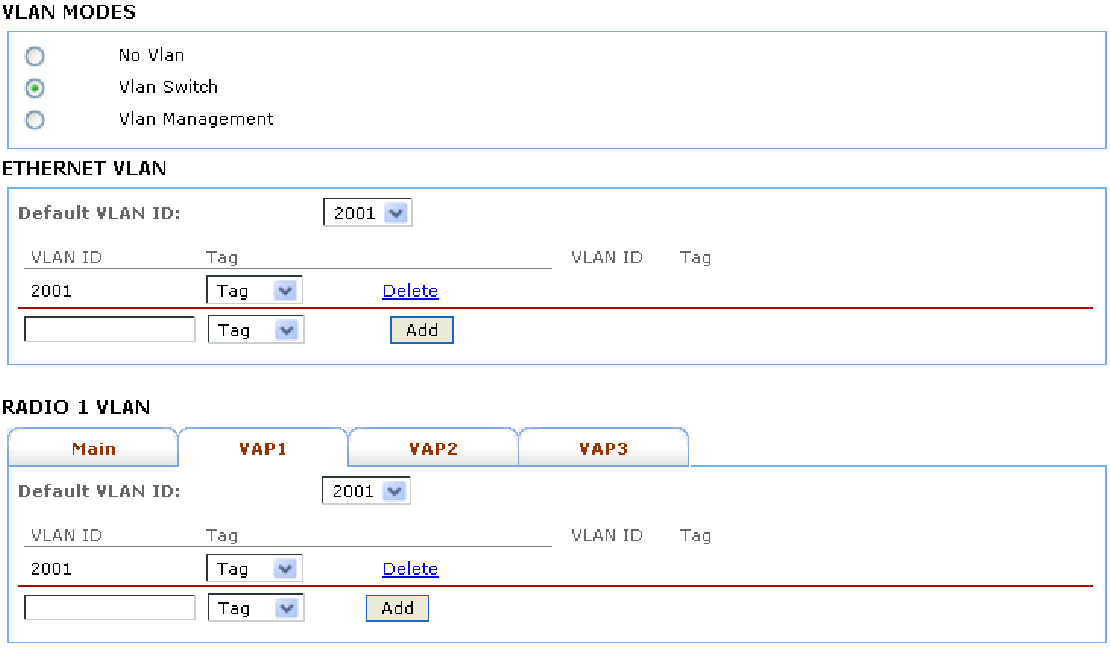
HOST NAME	IP ADDRESS	HARDWARE MAC	LEASE EXPIRED TIME
STATION-4	192.168.88.214	00-80-48-15-5D-E1	FRI DEC 31 17:03:32 1999

VLAN Tab

This setup lets you create virtual local network connection through the device Ethernet only and over wireless connections.
By default **VLAN** mode is disabled and checked on **No Vlan**

VLAN Switch

To setup VLAN network check on **Vlan Switch**



VLAN MODES

○ No Vlan
● Vlan Switch
○ Vlan Management

ETHERNET VLAN

Default VLAN ID: 2001

VLAN ID	Tag		VLAN ID	Tag
2001	Tag	Delete		
	Tag	Add		

RADIO 1 VLAN

Default VLAN ID: 2001

VLAN ID	Tag		VLAN ID	Tag
2001	Tag	Delete		
	Tag	Add		

To add a Tag VLAN ID for Ethernet port, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for MAIN wireless SSID, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for VAP1 wireless SSID, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for VAP2 wireless SSID, type in the ID number select **Tag** and click **Add**
To add a Tag VLAN ID for VAP3 wireless SSID, type in the ID number select **Tag** and click **Add**

*** **Warning:** Adding a Tag VLAN ID to device interface port can cause lost of connection to device web manager if the PC Ethernet port or wireless connection do not have a Tag VLAN ID or do not have the same Tag VLAN ID setup in device.
If this happened, use the device Reset button to clear the config and reconfigure.
Refer Reset button operations section.

Similarly, to add an untag VLAN ID enter the ID number and select **Untag** and click **Add**

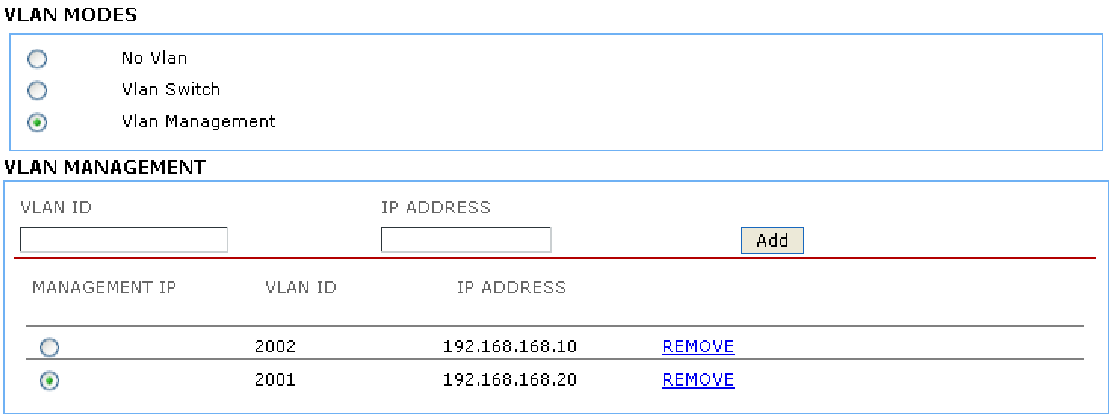
Refer to **Appendix V** for VLAN setup examples.

VLAN Management

Vlan management lets you control and limit only clients connection of same tag vlan ID group be open AP device web page.

*** Note:-**

Vlan Management works only in tag vlan pass-through mode. i.e. Vlan Switch is disabled. When Vlan Switch is enabled or configured, Vlan Management function stops operation.



VLAN MODES

○ No Vlan
○ Vlan Switch
● Vlan Management

VLAN MANAGEMENT

VLAN ID [ ] IP ADDRESS [ ]

MANAGEMENT IP	VLAN ID	IP ADDRESS	
○	2002	192.168.168.10	REMOVE
●	2001	192.168.168.20	REMOVE

Example:
Assuming there are 2 VLAN ID groups, 2001 and 2002 setup in AP device.
One entry in Vlan Management has Vlan ID 2001 with masquerade IP address 192.168.168.20
Another entry in Vlan Management has Vlan ID 2002 with masquerade IP address 192.168.168.10
You can only select one of the 2 entries to be the active Vlan ID and IP address.
If Vlan ID 2001 group is selected, then only computers in that Vlan ID group can open the AP device web page using the IP address, http://192.168.168.20
To change to other ID group say, Vlan ID 2002, mark the radio button under Management IP, then click Apply and Saved.

If there is no entry in Vlan Management, there is no restriction. All computers can open the AP device web page by the default IP address setup in Basic Network page.

Appendix I - Network

This section provides more detailed explanation on the network operation modes in general.

The Network Page allows the administrator to setup bridge or routing functionality.
Device can operate in bridge or router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the Network menu to configure the IP settings.

Network Mode Selections

Network Mode: Specify the operating network mode for the device.
The mode depends on the network topology requirements:

Bridge operating mode is selected by default as it is widely used by the subscriber stations, while connecting to Access Point or using WDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional Firewall settings can be configured for Layer 2 packet filtering and access control in Bridge mode.

Router operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on different IP subnet.
Router mode will block broadcasts while it is not transparent.

Device supports Multicast packet pass-through in Router mode. Router can act as DHCP server and use Network Address Translation (Masquerading) feature which is widely used by the Access Points. NAT will act as the firewall between LAN and WLAN networks. Additional Firewall settings can be configured for Layer 3 packet filtering and access control in Router mode.

Bridge Mode

Bridge Mode Network Settings

In bridge mode the device forwards all the network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment which has the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports. The bridge has assigned IP settings for management purposes:

Bridge IP Address:

The device can be set for static IP or can be set to obtain an IP address from the DHCP server it is connected to. One of the IP assignment modes must be selected:

DHCP: choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.

STATIC: choose this option to assign the static IP settings for the bridge interface.

IP Address: enter the IP address of the device while Static Bridge IP Address mode is selected. This IP will be used for the device management purposes.

IP Address and Netmask settings should consist with the address space of the network segment where device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the device will become unreachable.

Netmask: This is a value which when expanded into binary provides a mapping to define which portions of IP address groups can be classified as host devices and network devices.

Netmask defines the address space of the network segment where device resides. 255.255.255.0 (or /24) Netmask is commonly used among many C Class IP networks.

Gateway IP: Typically, this is the IP address of the host router which provides the point of connection to the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. Device will direct the packets of data to the gateway if the destination host is not within the local network. Gateway IP address should be from same address space (on same network segment) as the device.

Primary/Secondary DNS IP:

The Domain Name System (DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses of where the device looks for the translation source.

Primary DNS server IP address should be specified for the device management purposes.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

DHCP Fallback IP:

When device is placed in Dynamic IP Address mode (DHCP Client) and is unable to obtain an IP address from a valid DHCP server, it will fallback to the static IP address listed here. In case the IP settings of the devices are unknown, they can be access with the help of the u*Config utility*.

The u*Config Utility* should be started on the administrator PC which resides on the same network segment as the device.

Device will return to the default IP configuration (192.168.168.1/255.255.255.0) if the *Reset to defaults* routine is initiated.

Spanning Tree Protocol:

Multiple interconnected bridges create larger networks using the IEEE 802.1d Spanning Tree Protocol (STP), which is used for finding the shortest path within network and to eliminate loops from the topology.

If the STP is turned on, the Bridge device will communicate with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). STP should be turned off (selected by default) when the device is the only bridge on the LAN or when there are no loops in the topology as there is no sense for the bridge to participate in the Spanning Tree Protocol in this case.

Bridge mode Firewall Configuration Settings

Firewall functionality on bridge interface can be enabled using the "Enable Firewall" option. Bridge Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the "Configure" button.

Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN or LAN) where filtering of the incoming/passing-through packets is processed;

IP Type sets which particular L3 protocol type (ICMP, TCP, UDP, P2P) should be filtered;

Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;

Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;

Destination IP/mask is the destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;

Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.

Comments are the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.

On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during the system operation.

New Firewall entries can be saved by activating Apply button or discarded by activating Cancel button in the Firewall configuration window.

All the active firewall entries are stored in the FIREWALL chain of the ebtables filter table, while the device is operating in Bridge mode.

Click Apply Setting and Save Changes button to save the changes made in the Network page.

Appendix II – Wireless with Router Mode

This section provides more details on wireless with router function.

The role of the LAN and WLAN interface will change accordingly to the **Wireless Mode** while the device is operating in **Router** mode:

- Wireless interface and all the wireless clients connected are considered as the internal LAN and the Ethernet interface is dedicated for the connection to the external network while the device is operating in AP/AP WDS wireless mode;
- Wireless interface and all the wireless clients connected is considered as the external network and the all the network devices on LAN side as well as the Ethernet interface itself is considered as the internal network while the device is operating in Station/Station WDS mode.

Wireless/wired clients are routed from the internal network to the external one by default. Network Address Translation (NAT) functionality works the same way.

AP-Router mode Network Settings

IP Address: This IP addresses represents the LAN or WLAN interface which is connected to the internal network according to the wireless operation mode described above. IP will be used for routing in internal network (it will be the Gateway IP for all the devices connected on the internal network). IP address also will be used for the management purpose of the device.

WLAN IP Address: This IP addresses represents the LAN or WLAN interface which is connected to the external network according to the wireless operation mode described above. This is the IP address can be used for the routing and the device management purposes. The external network interface can be set for static IP or can be set to obtain an IP address from the DHCP server which should reside in the external network. One of the IP assignment modes must be selected for the external network interface:

DHCP – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external DHCP server.

PPPoE – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external PPPoE server.

Static – choose this option to assign the static IP settings for the external interface.

IP Address and Netmask settings should consist with the address space of the network segment where the device resides. If the device IP settings and administrator PC (which is connected to the device through wired or wireless) IP settings will use different address space, the device will become unreachable.

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Gateway IP: This is the IP address of the host router which resides on the external network and provides the point of connection to the next hop towards the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The device will direct all the packets to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the device's external network interface (Wireless interface in the Station case and the LAN interface in the AP case).

Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the device.

Primary DNS server IP is mandatory. It is used by the DNS Proxy and for the device management purpose.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on it's local network while the device is operating in AP/AP WDS wireless mode and in the contrariwise direction in "Station/Station WDS" mode.

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table, while the device is operating in Router mode. Please refer to the iptables tutorial for detailed description of the NAT functionality in Router mode.

Static routes should be specified in order the packets should pass-through the based device if the NAT is disabled in while operating in Router network mode.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients which will associate to the wireless interface while the device is operating in AP/AP WDS wireless mode and assigns IP addresses to clients which will connect to the LAN interface while the device is operating in Station/Station WDS mode.

Range Start/End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server.

DHCP Fallback IP: In case the external network interface of the Router is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here. In case the IP settings of the device are unknown, they can be retrieved with the help of the UConfig utility and should be started on the administrator PC which resides on the same network segment as the device.

Port Forwarding Settings

Port Forwarding: Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for number of applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port. Port Forwarding rules can be set in Port Forwarding window, which is opened by enabling the Port Forwarding option and activating the Configure button.

Port Forwarding entries can be specified by using the following criteria:

Private IP is the IP of the host which is connected to the internal network and needs to be accessible from the external network;

Private Port is the TCP/UDP port of the application running on the host which is connected to the internal network. The specified port will be accessible from the external network;

Type is the L3 protocol (IP) type which needs to be forwarded from the internal network.

Public Port is the TCP/UDP port of the based device which will accept and forward the connections from the external network to the host connected to the internal network.

Comments are the informal field for the comment of the particular port forwarding entry.

Few words about the particular port forwarding entry purpose are saved there usually.

Enabled flag enables or disables the effect of the particular port forwarding entry.

All the added firewall entries are saved in system configuration file, however only the enabled port forwarding entries will be active during the system operation.

New entries in port forwarding can be saved by activating Save button or discarded by activating Cancel button in the Port Forwarding configuration window.

DNS Proxy: The DNS Proxy forwards the Domain Name System requests from the hosts which reside in the internal network to the DNS server while device is in operating in Router mode. Valid Primary DNS Server IP needs to be specified for DNS Proxy functionality. Internal network interface IP of the device should be specified as the DNS server in the host configuration in order DNS Proxy should be able to get the DNS requests and translate domain names to IP addresses afterwards.

Bridge mode Firewall Configuration Settings

Firewall functionality on any router interface can be enabled using the "Enable Firewall" option. Router Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the "Configure" button.

Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed;

IP Type sets which particular L3 protocol type (ICMP, TCP, UDP, P2P) should be filtered;

Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;

Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;

Destination IP/mask is the destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;

Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.

Comments are the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.

On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during device operation.

New entries in Firewall can be saved by activating Apply Setting and Save Changes button or discarded by activating Cancel button in the Firewall configuration window.

All the active firewall entries are stored in the FIREWALL chain of the iptables filter table, while the device is operating in Router mode.

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers.

Select the IP Address option PPPoE to configure a PPPoE tunnel in order to connect to an ISP. Only the external network interface can be configured as PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. Broadcast address is used for the PPPoE server discovery and tunnel establishment.

Valid authorization credentials are required for the PPPoE connection:

PPPoE Username – username to connect to the server (must match the configured on the PPPoE server);

Password – password to connect to the server (must match the configured on the PPPoE server);

PPPoE MTU/MRU – the size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP tunnel;

Enable DMZ: The Demilitarized zone (DMZ) can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.

DMZ Management Port: Web Management Port for the based device (TCP/IP port 80 by default) will be used for the host device if DMZ Management Port option is enabled. In this case device will respond to the requests from the external network as if it was the host which is specified with DMZ IP. It is recommended to leave Management Port disabled while the based device will become inaccessible from the external network if enabled.

DMZ IP: connected to the internal network host, specified with the DMZ IP address will be accessible from the external network.

With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts which need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however provides the multicast traffic pass-through functionality.

Click Change button to save the changes made in the Network page.

Appendix III- Advanced Settings

This section provides more explanation on advanced setting for routing and wireless settings.
The Advanced options page allows you to manage advanced settings that influence on the device performance and behavior. The advanced wireless settings are dedicated for more technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your device.

Advanced Wireless Setting

The 802.11a/g data rates include 6, 9, 12, 18, 24, 36, 48, 54Mbps.
The 802.11n data rates are the MCS (Modulation Coding Scheme) rates.

MCS0 to MCS7 are 802.11n rates, which uses only 1 Tx/Rx stream.
MCS8 to MCS15 are 802.11n rates, which uses 2 Tx/Rx streams.

The Rate Algorithm has a critical impact on performance in outdoor links as generally lower data rates are more immune to noise while higher rates are less immune, but are capable of higher throughput.

Rate Aggressiveness:
Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm. There are 2 scenarios that Rate Aggressiveness is useful. Environment might be noisy at times. Lower the throughput will ensure better stability. Rate Aggressiveness allows device to reduce the transmit rate, so range or power can be higher. Choose a range of value from -3,-2,-1. Environment might be free of interference. But the fully auto algorithm might give low throughput. Increase Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose a range of value from +3, +2, +1.
Noise Immunity option increases the robustness of the device to operate in the presence of noise disturbance which is usually generated by external 802.11 traffic sources, channel hopping signals and other interferes.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or word "off". The default value is 2347 which means that RTS is disabled.
RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.
System uses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending a RTS frame first while data is send only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word "off". Setting the Fragmentation Threshold too low may result in poor network performance.

The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

Station Isolation: This option allows packets only to be sent from the external network to the CPE and vice verse (applicable for AP/AP WDS mode only). If the Client Isolation is enabled wireless stations connected to the same AP will not be able to interconnect on both layer 2 (MAC) and layer 3 (IP) level. This is effective for the associated stations and WDS peers also.

Acknowledgement Timeout

Device has an auto-acknowledgement timeout algorithm which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user also has the ability to enter the value manually.

Distance: specify the distance value in miles (or kilometers) using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout: specify the ACK Timeout. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set timeout it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the timeout is set too short or too long, it will result poor connection and throughput performance.

Changing the ACK Timeout value will change the Distance to the appropriate distance value for the ACK Timeout.

Auto: Adjust control and enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above. It is not recommended to use Auto Adjust option for long range links if the signal level is low or the high level of interference is present.

If two or more stations are located at the considerably different distance from the Access Point, the highest ACK Timeout for the farthest station should be set at the AP side. It is not recommended to use Auto Adjust option for Point-to-Multipoint connections as it will not warrant highest network performance in all the use cases.

Signal Strength LED Settings

LED Thresholds Configuration

The LED's for signal strength on the device can be made to light on when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy a CPE without logging into the unit (i.e. for antenna alignment operation).

Signal LED Thresholds specify the marginal value of Signal Strength (dBm) which will switch on LEDs indicating signal strength:

> **LED 1** (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it.
> **LED 2** (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it.
> **LED 3** (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.
> **LED 4** (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.

Configuration example: if the Signal Strength fluctuates around RSSI 15-30, the LED Thresholds can be adjusted to the RSSI values 15, 20, 25, 30.

Appendix IV- Services

This section provides more details on the system management services.

Ping WatchDog

The ping watchdog sets the device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the device will automatically reboot. This option creates a kind of "fail-proof" mechanism.
Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

Enable Ping Watchdog: control will enable Ping Watchdog Tool.
IP Address To Ping: enter the target host IP address to monitor.
Ping Interval: specify time interval (in seconds) between to send the ICMP “echo requests”.
Startup Delay: specify initial time delay (in seconds) from device startup or reboot to start sending first ICMP “echo requests”. Minimum value is 60 seconds.
Failure Count To Reboot: specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Device contains an SNMP agent which allows it to communicate to SNMP manage applications for network provisioning.
SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

Enable SNMP Agent: control will enable SNMP Agent.
SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access for device that supports SNMP v1.
Contact: specify the identity or contact in case an emergency situation arise.
Location: specify the physical location of the device.

NTP Client, Web, Telnet, SSH Server

NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the device system time. System Time is reported next to the every System Log entry while registering system events if Log option is enabled.
Web Server: the following the device Web Server parameters can be set there:
Use Secure Connection (HTTPS): If checked Web server will use secure HTTPS mode. HTTP mode is selected by default.
Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.
Server Port: Web Server TCP/IP port setting while using HTTP mode.

Telnet Server: the following the device Telnet Server parameters can be set there:
Enable Telnet Server: Enables Telnet access to the device.
Server Port: Telnet service TCP/IP port setting.

SSH Server: the following the device SSH Server parameters can be set there:
Enable SSH Server: Enables SSH access to the device.
Server Port: SSH service TCP/IP port setting.

System Log

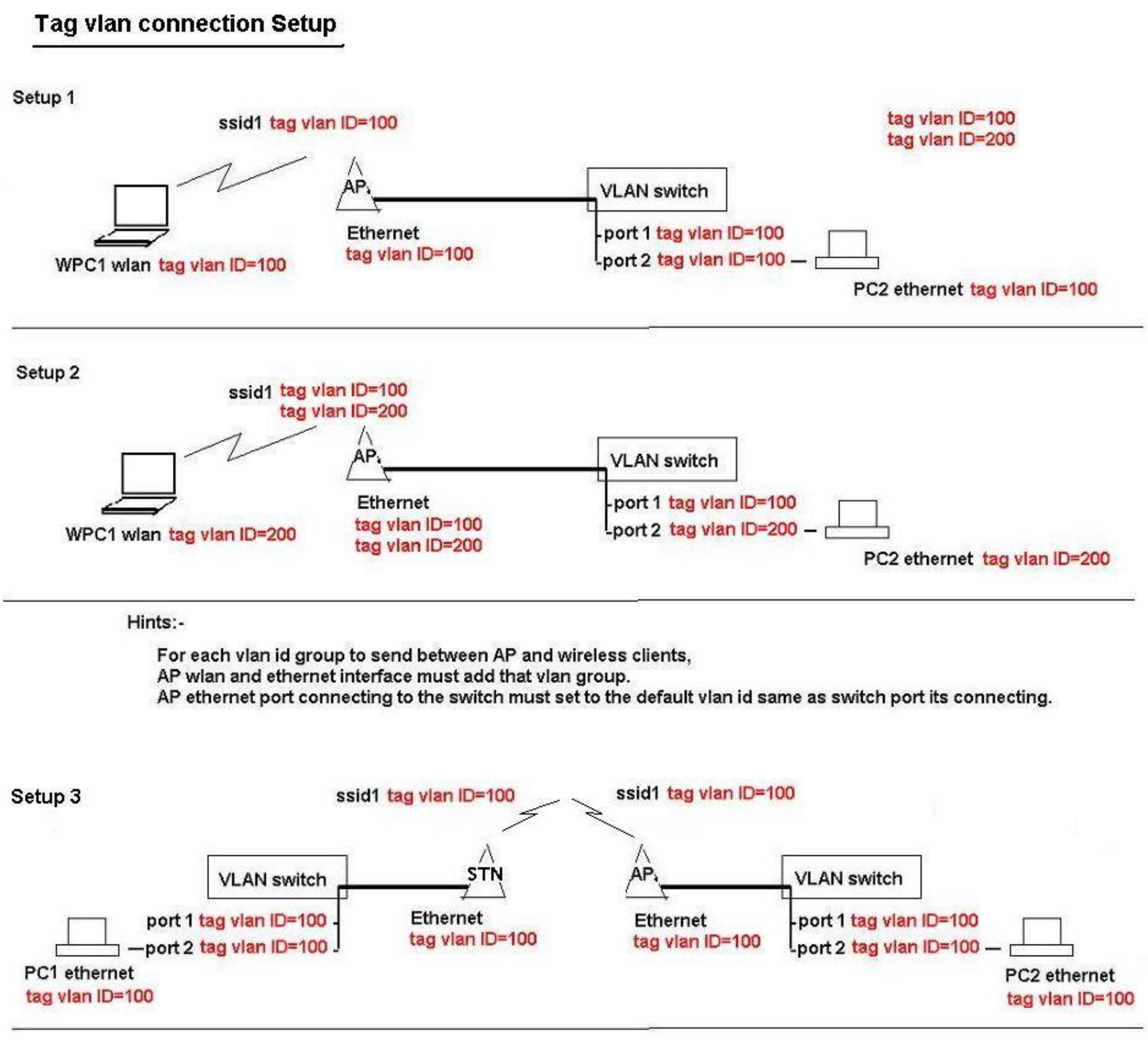
Enable Log : option enables the registration routine of the system log messages.
Enable Remote Log enables the syslog remote sending function while System log messages are sent to a remote server specified by the Remote Log IP Address and Remote Log Port.

Remote Log IP Address is the host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.
Remote Log Port is the TCP/IP port of the host syslog messages should be sent. "514" is the default port for the commonly used system message logging utilities
.

Every logged message contains at least a *System Time* and a Host Name. Usually a particular service name which generates the system event is specifies also within the message. Messages from different services have different context and different level of the details. Usually *error, warning* or *informational* system services messages are reported. The more detailed system messages are reported, the greater volume of log messages will be generated.

Appendix V- VLAN Setup examples

A) Tagged Wireless VLAN to Tagged Ethernet VLAN Setup

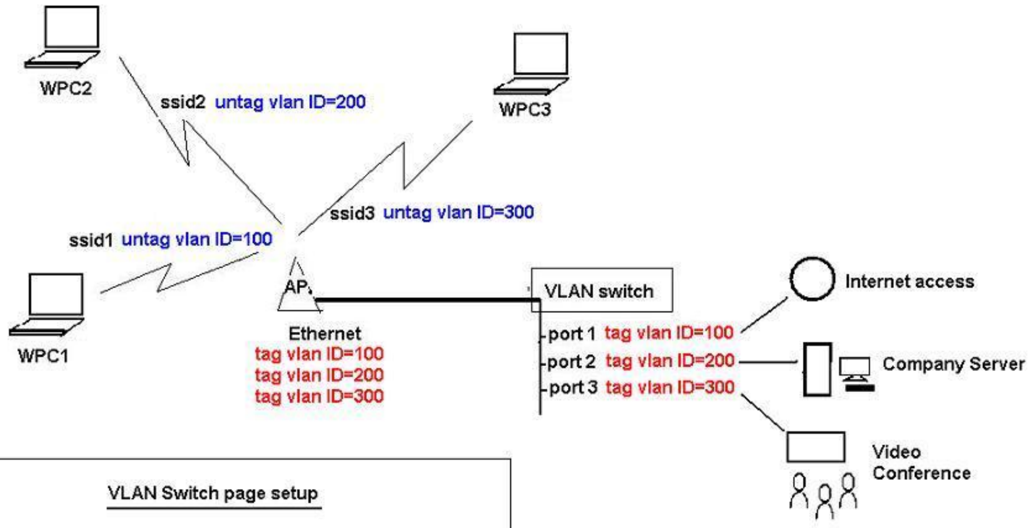


Hints:-

For each vlan id group to send between AP and wireless clients,
AP wlan and ethernet interface must add that vlan group.
AP ethernet port connecting to the switch must set to the default vlan id same as switch port its connecting.

B) Untagged Wireless VLAN to Tagged Ethernet VLAN setup

Multi-SSID with untag vlan connections to secured wired tag vlan network connections



VLAN Switch page setup

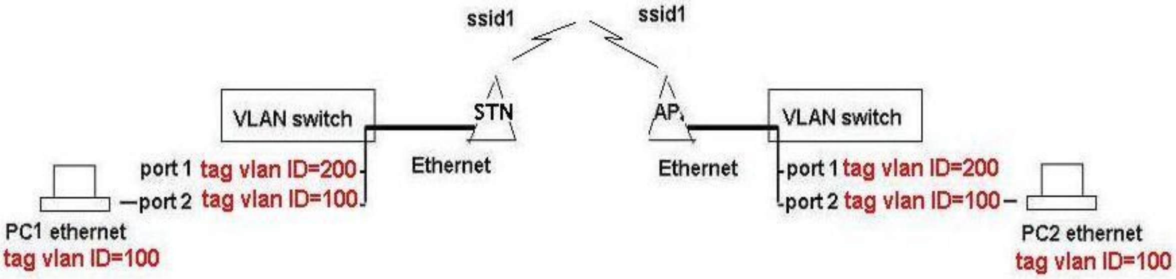
for wireless			for Ethernet port
MAIN	add	untag vlan ID=100	add tag vlan ID=100
VAP1	add	untag vlan ID=200	add tag vlan ID=200
VAP2	add	untag vlan ID=300	add tag vlan ID=300
VAP3	add	untag vlan ID=400	add tag vlan ID=400

C) Tagged VLAN Pass-Through

AP and Station link No VLAN Setup Required

Tagged VLAN pass-through. AP and Station link no VLAN Setup Required

* - AP and Station devices no VLAN setting required


ssid1
ssid1
VLAN switch
STN
AP
VLAN switch
port 1 tag vlan ID=200
port 2 tag vlan ID=100
Ethernet
Ethernet
port 1 tag vlan ID=200
port 2 tag vlan ID=100
PC1 ethernet
tag vlan ID=100
PC2 ethernet
tag vlan ID=100